Managing FDM Devices with Cisco Security Cloud Control

First Published: 2021-03-29

Last Modified: 2024-11-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 8 **Troubleshooting** 715

Managing FDM-Managed Devices with Cisco Security Cloud Control

Managing FDM-Managed Devices with Cisco Security Cloud Control

Important Secure Firewall device manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. Open a Support Ticket with TAC to enable this platform.

Cisco Security Cloud Control(formerly Cisco Defense Orchestrator) provides a simplified management interface and cloud-access to your Secure Firewall device manager devices. FDM-managed administrators will notice many similarities between the device interface and the Security Cloud Control interface. We built Security Cloud Control with the idea of keeping things as consistent as possible between managers.

Use Security Cloud Control to manage these aspects of your physical or virtual FDM-managed device:

- Onboard a Threat Defense Device
- Device Management
- Device Upgrade
- ASA to Threat Defense Migration
- Interface Management
- Routing
- High Availability
- Security Policies
- Promote Policy and Configuration Consistency
- Site-to-Site VPN

- Remote Access VPN
- Monitoring Your Network
- Cisco Security Analytics and Logging

Software and Hardware Support

Security Cloud Control supports version 6.4 and later, which can be installed on a number of different devices or virtual machines. See Secure Firewall Threat Defense Device Support Specifics for more information.

Managing Smart Licenses

You can use Cisco Smart Licenses to license the FDM-managed devices during onboarding or after onboarding the devices to Security Cloud Control. Smart Licensing is conveniently built into our workflows and easily accessible from the Security Cloud Control interface. For more information, see Applying or Updating a Smart License.

Note If the device you want to onboard is running software version 6.4 or 6.5, and is already smart-licensed, the device is likely to be registered with Cisco Smart Software Manager. **You must unregister the device from Cisco Smart Software Manager before you onboard it to Security Cloud Control with a registration Key.** When you unregister, the license and all optional licenses associated with the device, are freed in your virtual account.

If the device you want to onboard is running software version 6.6 and later and is already registered with the Cisco cloud, **you must unregister the device from Cisco Cloud Services before you onboard it to Security Cloud Control with a registration key.**

Security Cloud Control User Interfaces

Security Cloud Control GUI and CLI Interfaces

Security Cloud Control is a web-based management product that provides you with both a graphic user interface (GUI) and a command line interface (CLI) to manage your devices one at a time or many at once.

With the CLI interface, you can send commands to your FDM-managed devices directly from Security Cloud Control. Use CLI macros to save and run commonly used commands. See Command Line Interface Documentation and Security Cloud Control Command Line Interface, on page 543 for more information.

API Support

Security Cloud Control provides the API tool interface that can perform advanced actions on an FDM-managed device using the device's REST API. Additionally, this interface provides the following features:

- Records a history of already executed API commands.
- Provides system-defined API macros that can be reused.
- Allows creating user-defined API macros using the standard API macros, from a command you have already executed, or another user-defined macro.

For more information about the API tool, see Using the API Tool, on page 556.

Onboarding FDM-Managed Devices

Before you Onboard a Threat Defense Device, review the general device requirements and onboarding prerequisites.

The best practice is to onboard FDM-managed devices with a registration token. See Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key for more information.

You can use these additional methods to onboard an FDM-managed device to Security Cloud Control as well:

- Onboard an FDM-Managed Device Using Username, Password, and IP Address, on page 166
- Workflow and Prerequisites to Onboard the FDM-Managed Device Using Zero-Touch Provisioning
- Workflow and Prerequisites to Onboard the FDM-Managed Device Using Zero-Touch Provisioning, on page 177

Device Management

Use Security Cloud Control to upgrade software, configure high availability, configure device settings and network resources for your FDM-managed devices.

- **System Settings**. Once you have licensed your FDM-managed device and onboarded it, you can FDM-Managed Device Settings entirely from Security Cloud Control. You will be able to configure management access protocols, logging settings, DHCP and DNS server interaction, the device's hostname, the time server it uses, and URL filtering preferences.
- **Security Database Updates**. Keep your device up to date and compliant with current Update FDM-Managed Device Security Databases with a recurring task to check and update your device when necessary.
- **High Availability**. Manage HA configuration and operations with the Upgrade an FDM-Managed High Availability Pair.

Device Upgrade

Perform immediate upgrades to your FDM-managed devices, or schedule them, using one of following methods:

- Upgrade a Single FDM-Managed Device.
- Bulk FDM-Managed Devices Upgrade.
- Upgrade an FDM-Managed High Availability Pair.

ASA to Threat Defense Migration

Security Cloud Control helps you migrate your Adaptive Security Appliance (ASA) to an FDM-managed device. Security Cloud Control provides a wizard to help you migrate these elements of the ASA's running configuration to an Firewall device manager template:

This migration is supported for the following elements:

- Access Control Rules (ACLs)
- Interfaces
- Network Address Translation (NAT) rules

Managing FDM-Managed Devices with Cisco Security Cloud Control

- Network objects and network group objects
- Routes
- Service objects and service group objects
- Site-to-site VPN

See Migrating an ASA Configuration to an FDM-Managed Device Template for more information.

Interface Management

You can use Security Cloud Control to Configuring Firepower Interfaces on an FDM-managed device.

Routing

Routing is the act of moving information across a network from a source to a destination. Routing involves two basic activities: determining optimal routing paths and transporting packets through a network. Use Security Cloud Control to configure these aspects of routing:

- **Configuring Static Routes and Default Routes**. Using Security Cloud Control, you can Default Route, for your FDM-managed devices.
- **Bridge Group Support**. A bridge group is a virtual interface that groups one or more interfaces. The main reason to group interfaces is to create a group of switched interfaces. Using Security Cloud Control you can Configure a Bridge Group on your device.
- **NAT (Network Address Translation)**. NAT rules help route your traffic from your inside (private) network to the Internet. NAT rules also play a security role by keeping internal IP addresses hidden from the world outside your network. You can create and edit NAT rules for your device using Security Cloud Control. See Network Address Translation, on page 407 for more information.

Security Policies

Security policies examine network traffic with the ultimate goal of either allowing network traffic to reach or prevent network traffic from reaching its intended destination. Use Security Cloud Control to manage all the components of the device's security policies:

- **Copy and paste rules**. Make sharing rules across policies easy by copying and pasting rules from policy to another. See Copy FDM-Managed Access Control Rules for more information.
- **SSL Decryption Policy**. Some protocols, such as HTTPS, use Secure Sockets Layer (SSL) or its follow-on version, Transport Layer Security (TLS), to encrypt traffic for secure transmissions. Because the system cannot inspect encrypted connections, you must apply SSL decryption policy to decrypt them if you want to apply access rules that consider higher-layer traffic characteristics to make access decisions. See SSL Decryption Policy for more information.
- **Identity Policy**. Use Procedure to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group.
- **Security Intelligence Policy**. The Security Intelligence Policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. The system drops the traffic on the blocked list before evaluating it with the access control policy, thus reducing the amount of system resources used.

- **Access Control Policy**. The access control policy controls access to network resources by evaluating network traffic against access control rules. Secure Firewall Device Manager compares the criteria of the access control rules, in the order they appear in the access control policy, to the network traffic. When all the traffic conditions in an access control rule are matched, Secure Firewall Device Manager takes the action defined by the rule. You can Configure the FDM Access Control Policy using Security Cloud Control.
- TLS 1.3 Security Identity Discovery. Introduced in version 6.7, this feature allows you to perform URL filtering and application control on traffic encrypted with TLS 1.3. See Procedure for more information.
- **Intrusion Policy**. Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings. Intrusion policies are aspects of access control rules. See Intrusion Policy Settings in an FDM-Managed Access Control Rule for more information.

Note Snort 3 is available for FDM-managed devices running version 6.7 and later. Please note that you can toggle between Snort 2 and Snort 3 at will, but risk incompatible configurations. For more information about Snort 3, supported devices and software, and any limitations see Upgrade to Snort 3.0, on page 219.

- **Threat Events**. A Threat Events is a report of traffic that has been dropped, or that has generated an alert, after matching one of Cisco Talos's intrusion policies. In most cases, there's no need to tune IPS rules. If necessary, you have the option to override how an event is handled by changing the matching rule action in Security Cloud Control. Security Cloud Control supports IPS rule tuning on all versions of versions 6.4 and 6.6.1. Security Cloud Control does not support IPS rule tuning on any version 6.5, any 6.6 version other than 6.6.1, or any 6.7 version.
- **NAT (Network Address Translation)**. Order of Processing NAT Rules help route your traffic from your inside (private) network to the Internet. NAT rules also play a security role by keeping internal IP addresses hidden from the world outside your network. You can create and edit NAT rules for your Firepower Threat Defense using Security Cloud Control.

Promote Policy and Configuration Consistency

Object Management

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency because you can modify an object and that change affects all the other policies that use that object. Without objects, you would need to modify all the policies, individually, that require the same change.

Use Security Cloud Control to create and manage these Object Types:

- Create or Edit an Active Directory Realm Object
- Upload RA VPN AnyConnect Client Profile
- Application Filter Objects
- Certificate Objects
- DNS Group Objects

Managing FDM-Managed Devices with Cisco Security Cloud Control

- Geolocation Objects
- Configure Identity Sources for FDM-Managed Device
- Managing IKEv1 Policies
- Managing an IKEv1 IPsec Proposal Object
- Managing IKEv2 Policies
- Managing an IKEv2 IPsec Proposal Object
- Create or Edit a Firepower Network Object or Network Groups
- Create New RA VPN Group Policies
- Security Zone Object
- Service Objects
- Security Group Tags
- Create and Edit Syslog Server Objects
- Create or Edit an FDM-Managed URL Object

Resolve Object Issues

Security Cloud Control calls an object used on multiple devices a "shared object" and identifies them in the Objects page with this badge . Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices. Security Cloud Control makes it easy to Resolve Duplicate Object Issues, Resolve Unused Object Issues, and Resolve Inconsistent Object Issues to manage your devices as well as your repository of objects.

Templates

A Secure Firewall Device Manager template is a complete copy of an onboarded FDM-managed device's configuration. You can then modify that template and use it to configure other FDM-managed devices you manage. Secure Firewall Device Manager templates promote policy consistency between devices. See FDM-Managed Device Templates for more information.

High Availability

Security Cloud Control makes it easy to configure and manage a Create an FDM-Managed High Availability Pair. You can onboard an existing HA pair or create an HA pair in Security Cloud Control. HA configurations make it possible to maintain a secure network in scenarios where a device might be unavailable, such as during an upgrade period or an unexpected device failure; in failover mode, the standby device is already configured to become active, meaning that even if one of the HA devices becomes unavailable, the other device continues to handle traffic.

You can upgrade FDM-managed HA pairs in Security Cloud Control. See Upgrade an FDM-Managed High Availability Pair for more information.

Configuring Virtual Private Networks

Site-to-Site VPN

A virtual private network (VPN) consists of multiple remote peers transmitting private data securely to one another over an unsecured network, thusly connecting network to network. Security Cloud Control uses tunnels to encapsulate data packets within normal IP packets for forwarding over IP-based networks, using encryption to ensure privacy and authentication to ensure data integrity. See Introduction to Site-to-Site Virtual Private Network for more information.

For additional information about Virtual Private Networks, refer to the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Remote Access VPN

Remote Access (RA) VPN allows individuals to establish a secure connection to your network using supported laptop, desktop, and mobile devices. Security Cloud Control provides an intuitive user interface for you to setup RA VPN on FDM-managed devices. AnyConnect is the only client that is supported on endpoint devices for RA VPN connectivity to FDM-managed devices.

Security Cloud Control supports the following aspects of RA VPN functionality on FDM-managed devices:

- Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) for privacy, authentication, and data integrity
- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple FDM-managed devices

See Monitor Remote Access Virtual Private Network Sessions for more information. For additional information about Virtual Private Networks, refer to the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Monitoring Your Network

Security Cloud Control provides reports summarizing the impact of your security policies and methods of viewing notable events triggered by those security policies. Security Cloud Control also logs the changes you make to your devices and provides you with a way to label those changes so you can associate the work you do in Security Cloud Control with a help ticket or other operational request.

Executive Summary Report

Executive summary reports display a collection of operational statistics such as encrypted traffic, intercepted threats, detected web categories, and more. Data in the reports is generated when network traffic triggers an access rule or policy on an FDM-managed device. We recommend enabling malware and licenses, as well as enabling file logging for access rules, to allow a device to generate the events that are reflected in the reports.

Read FDM-Managed Device Executive Summary Report for more information about what the report offers and how you can use it to improve your network infrastructure. To create and manage your reports, see Monitoring and Reporting Change Logs, Workflows, and Jobs.

Managing FDM-Managed Devices with Cisco Security Cloud Control

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your FDM-managed devices and view them in one place in Security Cloud Control.

The events are stored in the Cisco cloud and viewable from the Event Logging page in Security Cloud Control where you can filter and review them to gain a clear understanding of what security rules are triggering in your network. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Firewall Analytics and Monitoring** package, the system can apply Secure Cloud Analytics dynamic entity modeling to your FDM-managed device events, and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your FDM-managed device events and your network traffic, and generates observations and alerts. You can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On. See About Security Analytics and Logging (SaaS) in Security Cloud Control for more information.

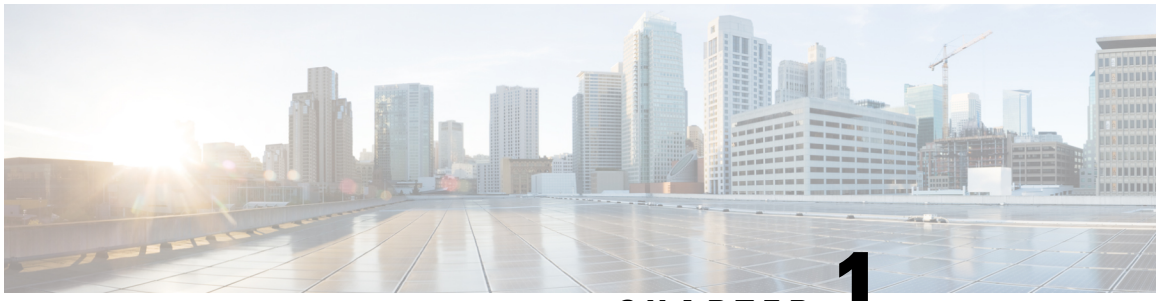
Change Log

The Manage Change Logs in Security Cloud Control, on page 585 continuously captures configuration changes as they are made in Security Cloud Control. This single view includes changes across all supported devices and services. These are some of the features of the change log:

- Side-by-side comparison of changes made to device configuration
- Plain-English labels for all change log entries.
- Records on-boarding and removal of devices.
- Detection of policy change conflicts occurring outside of Security Cloud Control.
- Answers who, what, and when during an incident investigation or troubleshooting.
- The full change log, or only a portion, can be downloaded as a CSV file.

Change Request Management

Change Request Management allows you to associate a change request and its business justification, opened in a third-party ticketing system, with an event in the Change Log. Use change request management to create a change request in Security Cloud Control, identify it with a unique name, enter a description of the change, and associate the change request with change log events. You can later search the Change Log for the change request name.



CHAPTER 1

Basics of Security Cloud Control

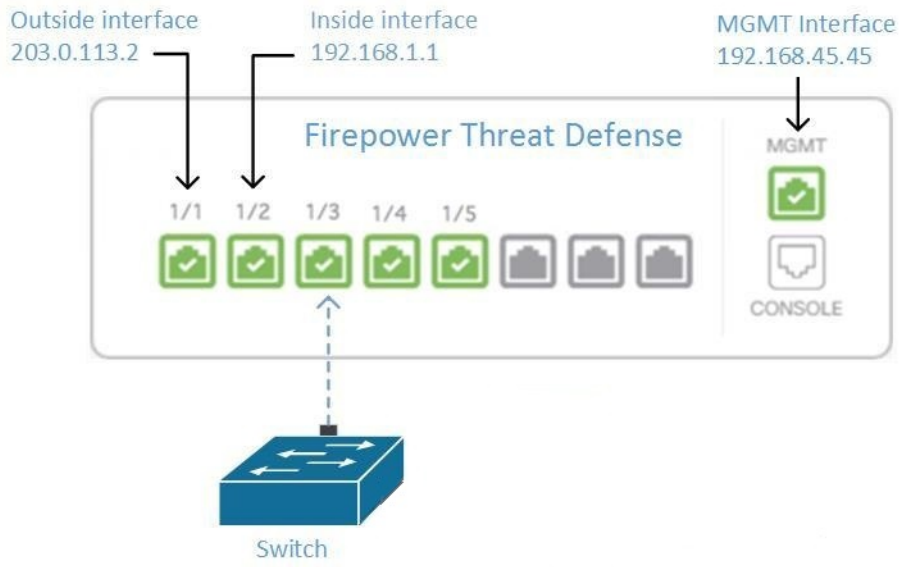
Security Cloud Control provides a unique view of policy management through a clear and concise interface. Below are topics that cover the basics of using Security Cloud Control for the first time.

Networking Requirements

Managing an FDM-Managed Device from the Inside Interface

Managing an FDM-managed device using the inside interface may be desirable if the dedicated MGMT interface is assigned an address that is not routable within your organization; for example, it might only be reachable from within your data center or lab.

Figure 1: Interface Addresses



Remote Access VPN Requirement

If the FDM-managed device you manage with Security Cloud Control will be managing Remote Access VPN (RA VPN) connections, Security Cloud Control must manage the device using the inside interface.

What to do next:

Continue to Manage an FDM-Managed Device from the Inside Interface, on page 2 for the procedure for configuring the FDM-managed device.

Manage an FDM-Managed Device from the Inside Interface

This configuration method:

- Assumes that the FDM-managed device has not been on-boarded to Security Cloud Control.
- Configures a data interface as the inside interface.
- Configures the inside interface to receive MGMT traffic (HTTPS).
- Allows the address of the cloud connector to reach the inside interface of the device.

Before you begin

Review the prerequisites for this configuration in these topics:

- Managing an FDM-Managed Device from the Inside Interface, on page 2
- Connect Security Cloud Control to your Managed Devices, on page 15

Procedure

Step 1 Log in to the Secure Firewall device manager.

Step 2 In the **System Settings** menu, click **Management Access**.

Step 3 Click the **Data Interfaces** tab and click **Create Data Interface**.

a. In the **Interface** field, select the pre-named "**inside**" interface from the list of interfaces.

b. In the **Protocols** field, select **HTTPS** if it is not already.

c. In the **Allowed Networks** field, select the network objects that represent the networks inside your organization that will be allowed to access the inside address of the FDM-managed device. The IP address of the SDC or cloud connector should be among the addresses allowed to access the inside address of the device.

In the Interface Addresses diagram, the SDC's IP address, 192.168.1.10 should be able to reach 192.168.1.1.

Step 4 **Deploy the change**. You can now manage the device using the inside interface.

What to do next

What if you are using a Cloud Connector?

Use the procedure above and add these steps:

- Add a step to "NAT" the outside interface to (203.0.113.2) to the inside interface (192.168.1.1). See Interface Addresses.
- In step 3c of the procedure above, your "Allowed Network" is a network group object containing the public IP addresses of the cloud connector.
- Add a step that creates an Access Control rule allowing access to the outside interface (203.0.113.2) from the public IP addresses of the cloud connector. See for a list of all the Cloud Connector IP addresses for the various Security Cloud Control regions.

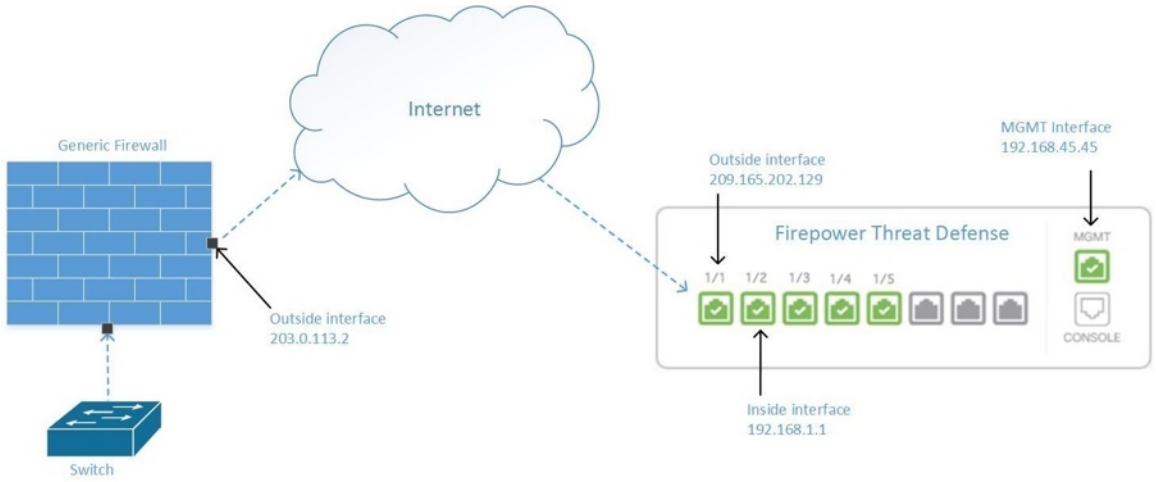
Onboard the FDM-Managed Device

The recommended way of onboarding the FDM-managed device to Security Cloud Control is to use the registration token onboarding approach. After you configure the inside interface to allow management access from the Cloud Connector to the FDM-managed device, onboard the FDM-managed device with the user name and password. See Onboard a Threat Defense Device for more information. You will connect using the IP address of the inside interface. In our scenario above, that address is 192.168.1.1.

Managing an FDM-Managed Device from the Outside Interface

Managing an cloud-delivered Firewall Management Center device from the outside interface may be desirable if you have one public IP address assigned to a branch office and Security Cloud Control is managed using a Cloud Connector at another location.

Figure 2: Device Management on Outside Interface



This configuration doesn't mean that the physical MGMT interface is no longer the device's management interface. If you were in the office where the cloud-delivered Firewall Management Center device was located, you would be able to connect to the address of the MGMT interface and manage the device directly.

Remote Access VPN Requirement

If the device you manage with cloud-delivered Firewall Management Center will be managing Remote Access VPN (RA VPN) connections, cloud-delivered Firewall Management Center will not be able to manage the cloud-delivered Firewall Management Center device using the outside interface. See Managing an FDM-Managed Device from the Inside Interface instead.

What to do next:

Continue to Manage the FDM-Managed Device's Outside Interface, on page 4 for the procedure for configuring the cloud-delivered Firewall Management Center device.

Manage the FDM-Managed Device's Outside Interface

This configuration method:

1. Assumes that the FDM-managed device has not been on-boarded to Security Cloud Control.
2. Configures a data interface as the outside interface.
3. Configures management access on the outside interface.
4. Allows the public IP address of the cloud connector (after it has been NAT'd through the firewall) to reach the outside interface.

Before you begin

Review the prerequisites for this configuration in these topics:

- Manage the FDM-Managed Device's Outside Interface, on page 4
- Connect Security Cloud Control to your Managed Devices, on page 15

Procedure

Step 1 Log in to the Secure Firewall device manager.

Step 2 In the **System Settings** menu, click **Management Access**.

Step 3 Click the **Data Interfaces** tab and click **Create Data Interface**.

a. In the **Interface** field, select the pre-named "**outside**" interface from the list of interfaces.

b. In the **Protocols** field, select **HTTPS** if it is not already. Security Cloud Control only needs HTTPS access.

c. In the **Allowed Networks** field, create a host network object containing the public-facing IP address of the cloud connector after it gets NAT'd through the firewall.

In the Device Management from Outside Interface network diagram, the cloud connector's IP address, 10.10.10.55, would be NAT'd to 203.0.113.2. For the Allowed Network, you would create a host network object with the value 203.0.113.2.

Step 4 Create an Access Control policy in Secure Firewall device manager that allows management traffic (HTTPS) from the public IP address of the SDC or cloud connector, to the outside interface of your FDM-managed device. In this scenario, the source address would be 203.0.113.2 and the source protocol would be HTTPS; the destination address would be 209.165.202.129 and the protocol would be HTTPS.

Step 5 **Deploy the change**. You can now manage the device using the outside interface.

What to do next

What if you are using a cloud connector?

The process is very similar, except for two things:

- In step 3c of the procedure above, your "Allowed Network" is a network group object containing the public IP addresses of the cloud connector. See Connecting Devices to Security Cloud Control Through the Cloud Connector for a list of Cloud Connector IP addresses for the various Security Cloud Control regions.
- In step 4 of the procedure above, you create an Access Control rule that allows access to the outside interface from the public IP addresses of the cloud connector.

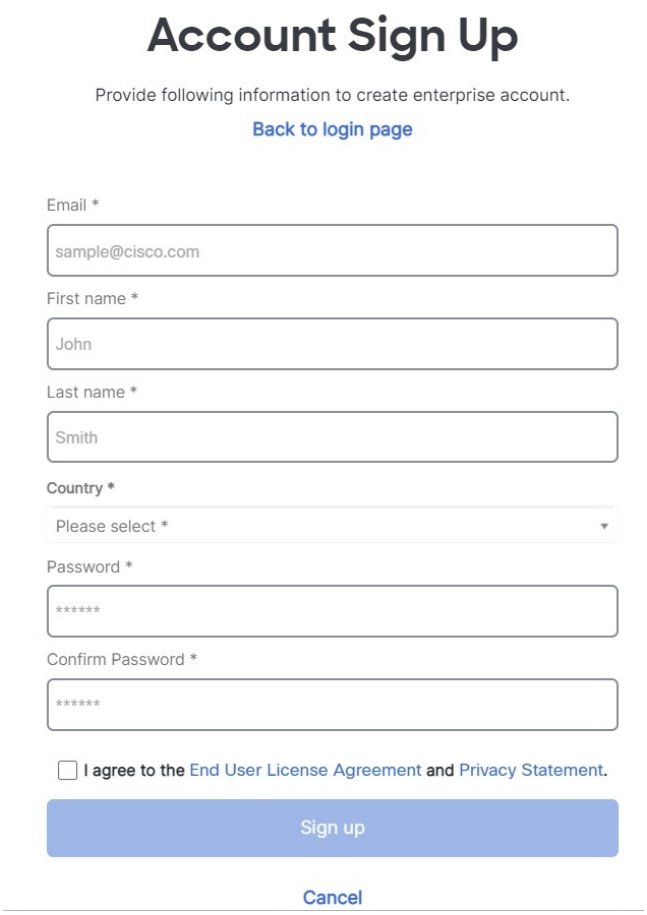
The Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key approach is the recommended way of onboarding the FDM-managed device to Security Cloud Control. After you configure the outside interface to allow management access from the cloud connector, onboard the FDM-managed device. You will connect using the IP address of the outside interface. In our scenario, that address is 209.165.202.129.

Create a Security Cloud Control Tenant

You can provision a new Security Cloud Control tenant to onboard and manage your devices. If you use an On-Premises Firewall Management Center Version 7.2 and later, and want to integrate it with the Cisco Security Cloud, you can also create a Security Cloud Control tenant as part of the integration workflow.

Procedure

1. Go to https://manage.security.cisco.com/provision.
2. Select the region where you want to provision your Security Cloud Control tenant and click **Sign Up**.
3. On the **Security Cloud Sign On** page, provide your credentials.
4. If you do not have a Security Cloud Sign On account and want to create one, click **Sign up now**.
   a. Provide the information to create an account.



Here are some tips:

- **Email**: Enter the email address that you will eventually use to log in to Security Cloud Control.
- **Password**: Enter a strong password.

b. Click **Sign up**. Cisco sends you a verification email to the address you registered with.

c. Open the email and click **Activate account** both on the mail and the **Security Cloud Sign On** page.

d. Configure multifactor authentication using Duo on a device of your choice and click **Log in with Duo** and **Finish**.

Note We recommend installing the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.

5. Provide a name for your tenant and click **Create new account**.
6. A new Security Cloud Control tenant is created in the region you have chosen; you will also receive an e-mail about your Security Cloud Control tenant being created, with the details. If you are associated with multiple Security Cloud Control tenants already, on the **Choose a tenant** page, select the tenant you just created to log in to it. If you have created a new Security Cloud Control tenant for the first time, you get logged into your tenant directly.

   For information about logging on to your Security Cloud Control tenant for the first time, see Initial Login to Your New Security Cloud Control Tenant.

   For information about managing a Security Cloud Control tenant and various tenant settings, see Tenant Management.

Upgrade your Security Cloud Control tenant to full version

If you are using a free trial version of Security Cloud Control, you will keep seeing the **You are in a free trial of** Security Cloud Control banner, with the number of days left in the trial period. You can choose to upgrade your Security Cloud Control tenant to full version any time during the trial period. Contact your Cisco sales representative or contact Cisco Sales, and they can place an order on your behalf and get you the sales order number.

Once you obtain the sales order number, click **Upgrade to full version** on the banner and enter the order number to begin using the full version of Security Cloud Control.

Request Security Cloud Control trial period extension

If you want to continue using the trial version for 30 days, click **Request for an extension**.

Sign in to Security Cloud Control

To log in toSecurity Cloud Control, a customer needs an account with a SAML 2.0-compliant identity provider (IdP), a multi-factor authentication provider, and Manage Users in Security Cloud Control.

The IdP account contains the user's credentials and the IdP authenticates the user based on those credentials. Mutli-factor authentication provides an added layer of identity security. The Security Cloud Control user record primarily contains the username, the Security Cloud Control tenant with which they are associated, and the user's role. When a user logs in, Security Cloud Control tries to map the IdP's user ID to an existing user record on a tenant in Security Cloud Control. The user is logged in to that tenant when Security Cloud Control finds a match.

Unless your enterprise has its own single sign-on identity provider, your identity provider is Security Cloud Sign On. Security Cloud Sign On uses Duo for multi-factor authentication. Customers can Integrate Your SAML Single Sign-On with Security Cloud Control if they choose.

To log into Security Cloud Control, you must first create an account in Cisco Security Cloud Sign On, configure multi-factor authentication (MFA) using Duo Security and have your tenant Super Admin create a Security Cloud Control record.

On October 14, 2019, Security Cloud Control converted all previously-existing tenants to use Cisco Security Cloud Sign On as their identity provider and Duo for MFA.

Note

- If you sign in to Security Cloud Control using your own single sign-on identity provider, the transition to Cisco Security Cloud Sign On did not affect you. You continue to use your own sign-on solution.
- If you are in the middle of a free trial of Security Cloud Control, this transition did affect you.

If your Security Cloud Control tenant was created on or after October 14, 2019, see Initial Login to Your New Security Cloud Control Tenant, on page 8.

If your Security Cloud Control tenant existed before October 14, 2019, see Migrate to Cisco Security Cloud Sign On Identity Provider, on page 9.

Initial Login to Your New Security Cloud Control Tenant

Before You Begin

Install DUO Security. We recommend installing the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.

Time Synchronization. You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock set automatically or manually set it to the correct time.

Security Cloud Control uses Cisco Security Cloud Sign On as its identity provider and Duo for multi-factor authentication (MFA). . If you do not have a Cisco Security Cloud Sign On account, when you create a new Security Cloud Control tenant using https://manage.security.cisco.com/provision, the provisioning flow involves various steps, including creating a Security Cloud Sign On account and configuring MFA using Duo.

MFA provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into Security Cloud Control. The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand.

Important

If your Security Cloud Control tenant existed before October 14, 2019, use Migrate to Cisco Security Cloud Sign On Identity Provider, on page 9 for log in instructions instead of this article.

What to do next?

Continue to, Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication, on page 78. It is a four-step process. You need to complete all four steps.

Signing in to Security Cloud Control in Different Regions

These are the URLs you use to sign in to Security Cloud Control in different AWS regions:

Table 1: Security Cloud Control URLs in Different Regions

Region	Security Cloud Control URL
Asia-Pacific and Japan (APJ)	https://apj.manage.security.cisco.com
Australia (AUS)	https://au.manage.security.cisco.com
Europe, the Middle East, and Africa (EMEA)	https://eu.manage.security.cisco.com
India (IN)	https://in.manage.security.cisco.com
United States (US)	https://us.manage.security.cisco.com

Troubleshooting Login Failures

Login Fails Because You are Inadvertently Logging in to the Wrong Security Cloud Control Region

Make sure you are logging into the appropriate Security Cloud Control region. After you log into https://sign-on.security.cisco.com, you will be given a choice of what region to access.

See Signing in to Security Cloud Control in Different Regions, on page 9 for information about which region you shoud sign into.

Migrate to Cisco Security Cloud Sign On Identity Provider

On October 14, 2019,Security Cloud Control converted all tenants to Cisco Security Cloud Sign On as their identity provider and Duo for multi-factor authentication (MFA). **To log into Security Cloud Control, you must first activate your account in Cisco Secure Sign-On and configure MFA using Duo**.

Security Cloud Control requires MFA which provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into Security Cloud Control. The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand.

Note

- If you sign in to Security Cloud Control using your own single sign-on identity provider, this transition to Cisco Security Cloud Sign On and Duo does not affect you. You continue to use your own sign-on solution.
- If you are in the middle of a free trial of Security Cloud Control, this transition does apply to you.
- **If your Security Cloud Control tenant was created on or after October 14, 2019**, see Initial Login to Your New Security Cloud Control Tenant, on page 8 for log in instructions instead of this article.

Before You Begin

We strongly recommend the following steps prior to migrating:

- **Install DUO Security.** We recommend installing the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.
- **Time Synchronization**. You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock set automatically or manually set it to the correct time.
- Create a New Cisco Secure Sign-On Account and Configure Duo Multi-factor Authentication. It is a four-step process. You need to complete all four steps.

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

Solution If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try "forgot password" cannot recover a viable password, you may have tried to login without creating a new Cisco Security Cloud Sign On account, you need to sign up for a new Cisco Security Cloud Sign On Account by following the instructions in Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication, on page 78.

Login to the Cisco Security Cloud Sign On Dashboard Succeeds but You Can't Launch Security Cloud Control

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control and Cisco Secure Sign-On.

Login Fails Using a Saved Bookmark

Solution You may be attempting to log in using an old bookmark you saved in your browser. The bookmark could be pointing to https://cdo.onelogin.com.

Solution Log in to https://sign-on.security.cisco.com.

- **Solution** If you have not yet created a Cisco Secure Sign-On account, Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication.

- **Solution** If you have created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Security Cloud Control APJ
  - **Solution** Cisco Security Cloud Control Australia
  - **Solution** Cisco Security Cloud Control EU
  - **Solution** Cisco Security Cloud Control India
  - **Solution** Cisco Security Cloud Control US
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Launch a Security Cloud Control Tenant

Procedure

Step 1 Click the appropriate Security Cloud Control button for your region on the Cisco Security Cloud Sign On dashboard.

Step 2 Click the authenticator logo to choose Duo Security or Google Authenticator if you have set up both authenticators.

- If you already have a user record on an existing tenant, you are logged into that tenant.
- If you already have a user record on several portals, you will be able to choose which portal to connect to.
- If you already have a user record on several tenants, you will be able to choose which Security Cloud Control tenant to connect to.
- If you do not already have a user record on an existing tenant, you will be able to learn more about Security Cloud Control or request a trial tenant.

The **Portals** view retrieves and displays consolidated information from multiple tenants. See Manage Multi-Tenant Portal, on page 66 for more information.

The **Tenant** view shows several tenants on which you have a user record.

Manage Super Admins on Your Tenant

It is a best practice to limit the number of Super Admins on your tenant. Determine which users should have Super Admin privileges, review Manage Users in Security Cloud Control, and change the roles of other users to "Admin."

Get Started With Security Cloud Control

The **Get started with Security Cloud Control** is an intuitive interface that guides you through sequential tasks for efficiently setting up and configuring your firewalls.

Sign in to Security Cloud Control and in the top menu, click ( ).

- The **On-premises management** page provides links to:
  - Onboard the threat defense device to the on-premises management center using Security Cloud Control.
  - Migrate a threat defense device that is managed by an on-premises management center to the cloud-delivered Firewall Management Center.
  - Perform bulk provisioning of multiple threat defense devices to the cloud-delivered Firewall Management Center using device templates.
  - Analyze your policies, detect anomalies, and receive curated remediation recommendations.
- The **Manage firewalls** page provides links to:
  - Onboard and manage threat defense, Cisco Secure Firewall ASA, and Meraki MX firewalls.

- Set up a site-to-site VPN connection.
- Leverage the Cisco AI Assistant to manage firewall policies and access-related documentation when needed.
- Subscribe to receive notifications for troubleshooting common issues.

- The **Protect cloud assets** page provides links to:
  - Safeguard your cloud assets by protecting data and applications across multicloud environments with consistent security measures using Multicloud Defense.

About Security Cloud Control Licenses

Security Cloud Control requires a base subscription for tenant entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control base subscriptions based on the number of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription gives you a Security Cloud Control tenant, and for every device you choose to manage using Security Cloud Control, you need separate device licenses.

For the purposes of planning your deployment, note that each Security Cloud Control tenant can manage approximately 500 devices through the Secure Device Connector (SDC) and any number of devices using the cloud connector. See Secure Device Connector (SDC) for more information.

To onboard and manage devices from Security Cloud Control, you need to purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Cisco Security Cloud Control subscriptions are term-based:

- **Base** - Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control tenant and onboard adequately licensed devices.
- **Device License** - Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control for three years, if you purchase a three-year software subscription to the Cisco Firepower 1010 device.

See Software and Hardware Supported by Security Cloud Control for more information on Cisco security devices that Security Cloud Control supports.

Important You do not require two separate device licenses to manage a high availabilty device pair in Security Cloud Control. If you have a Secure Firewall Threat Defense (FTD) high availability pair, purchasing one FTD device license is sufficient, as Security Cloud Control considers the pair of high availability devices as one single device.

Note You cannot manage Security Cloud Control licensing through the Cisco smart licensing portal.

Software Subscription Support

The Security Cloud Control base subscription includes software subcription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC), at no extra cost. While the software support is selected by default, you can also leverage the Security Cloud Control solution support based on your requirement.

Security Cloud Control Evaluation License

You can request for a 30-day Security Cloud Control trial from your SecureX account. See Request a Security Cloud Control Tenant for more information.

Cloud-Delivered Firewall Management Center and Threat Defense Licenses

You do not have to purchase a separate license to use the cloud-delivered Firewall Management Center in Security Cloud Control; the base subscription for a Security Cloud Control tenant includes the cost for the cloud-delivered Firewall Management Center.

Cloud-delivered Firewall Management Center Evaluation License

The cloud-delivered Firewall Management Center comes provisioned with a 90-day evaluation license, after which the threat defense services are blocked.

To learn how to get a cloud-delivered Firewall Management Center provisioned on your Security Cloud Control tenant, see Request a Cloud-delivered Firewall Management Center for your Security Cloud Control Tenant.

Note The cloud-delivered Firewall Management Center does not support specific license reservation (SLR) for devices in air-gapped networks.

Threat Defense Licenses for Cloud-Delivered Firewall Management Center

You need individual licenses for each Secure Firewall Threat Defense device managed by the cloud-delivered Firewall Management Center. See Licensing in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control* for information.

To know how Security Cloud Control handles licensing for the devices migrated to the cloud-delivered Firewall Management Center, see Migrate Threat Defense from Management Center to Cloud.

Secure Device Connector

The Secure Device Connector (SDC) is an intelligent proxy that allows your Cisco devices to communicate with Security Cloud Control. When onboarding a device that is not directly reachable over the internet to Security Cloud Control using device credentials, you can deploy an SDC in your network to proxy communications between the devices and Security Cloud Control. Alternatively, if you prefer, you can enable a device to receive direct communications through its outside interface from Security Cloud Control. Adaptive Security Appliances (ASA), Meraki MXs, Secure Firewall Threat Defense devices, and Secure Firewall Management Center devices, generic SSH and IOS devices, can all be onboarded to Security Cloud Control using an SDC.

The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices, and messages that need to be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control, sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control.

The SDC uses secure communication messages signed and encrypted using AES-128-GCM over HTTPS (TLS 1.3) to communicate with Security Cloud Control. All credentials for onboarded devices and services are encrypted directly from the browser to the SDC as well as encrypted at rest using AES-128-GCM. Only the SDC has access to the device credentials. No other Security Cloud Control service has access to the credentials. See Connect Security Cloud Control to your Managed Devices, on page 15 for information explaining how to allow communication between an SDC and Security Cloud Control.

The SDC can be installed on any Ubuntu instance. For convenience, we provide an OVA for a hardened Ubuntu 22 instance which includes the SDC CLI pre-installed. The CLI helps you configure your VM, install all required system packages, and bootstrap the SDC as a Docker container on the host. Alternatively, you can roll your own Ubuntu instance (versions 20 through 24 are currently tested) and download the CLI separately.

Each Security Cloud Control tenant can have an unlimited number of SDCs. These SDCs are not shared between tenants, they are dedicated to a single tenant. The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, expect one SDC to support approximately 500 devices.

Deploying more than one SDC for your tenant also provides these benefits:

- You can manage more devices with your Security Cloud Control tenant without experiencing performance degradation.
- You can deploy an SDC to an isolated network segment within your network and still manage the devices in that segment with the same Security Cloud Control tenant. Without multiple SDCs, you would need to manage the devices in those isolated network segments with different Security Cloud Control tenants.

Multiple SDCs can run on a single host, follow the bootstrap procedure for each SDC you want to run. The initial SDC on your tenant incorporates the name of your tenant and the number 1 and is displayed on the **Secure Connectors** tab in the **Services** page of Security Cloud Control. Each additional SDC is numbered in order.

For more information, see Deploy a Secure Device Connector Using Security Cloud Control's VM Image, on page 17 and Deploy a Secure Device Connector On Your VM, on page 21.

Related Information:

- Connect Security Cloud Control to your Managed Devices
- Update your Secure Device Connector, on page 34
- Remove a Secure Device Connector, on page 33

Connect Security Cloud Control to your Managed Devices

Security Cloud Control connects to the devices that it manages through the cloud connector or through a Secure Device Connector (SDC).

If your device can be accessed directly from the internet, you should be using the cloud connector to connect to your device. If you can, configure the device to allow inbound access on port 443 from the Security Cloud Control IP addresses in your cloud region.

If your device is not accessible from the internet, you can deploy an on-premises SDC in your network to allow Security Cloud Control to communicate with your devices.

Configure the device to allow full inbound access from your device subnets/IPs on port 443 (or whichever port you have configured for your device management).

An FDM-managed device can be onboarded to Security Cloud Control using its device credentials, a registration key, or its serial number whether it is directly accessible from the internet. If the FDM-managed device does not have direct access to the internet, but it resides on a network that does; the Security Services Exchange connector delivered as part of the device can reach the Security Services Exchange cloud allowing the FDM-managed device to be onboarded.

You need an on-premises SDC in your network to onboard:

- An FDM-managed device that is not accessible from the cloud and the credentials onboarding method is used.

All other devices and services do not require an on-premise SDC as Security Cloud Control will connect using its cloud connector. See the next section to know the IP addresses that must be allowed for inbound access.

Connecting Devices to Security Cloud Control Through the Cloud Connector

When connecting Security Cloud Control directly to your device through the cloud connector, you should allow inbound access on port 443 (or whichever port you have configured for your device management) for the various IP addresses in the EMEA, United States, or APJ region.

If you are a customer in the **Asia-Pacific-Japan (APJ)** region, and you connect to Security Cloud Control at https://apj.manage.security.cisco.com, allow inbound access from the following IP addresses:

- 54.199.195.111
- 52.199.243.0

If you are a customer in the **Australia (AUS)** region, and you connect to Security Cloud Control at https://au.manage.security.cisco.com, allow inbound access from the following IP addresses:

- 13.55.73.159
- 13.238.226.118

If you are a customer in **Europe, the Middle East, or Africa (EMEA)** region, and you connect to Security Cloud Control at https://eu.manage.security.cisco.com, allow inbound access from the following IP addresses:

- 35.157.12.126
- 35.157.12.15

If you are a customer in the **India (IN)** region, and you connect to Security Cloud Control at https://in.manage.security.cisco.com, allow inbound access from the following IP addresses:

- 35.154.115.175
- 13.201.213.99

If you are a customer in the **United States (US)** region, and you connect to Security Cloud Control at https://us.manage.security.cisco.com, allow inbound access from the following IP addresses:

- 52.34.234.2

- 52.36.70.147

Connecting Security Cloud Control to SDC

When connecting Security Cloud Control to your device through an SDC, the devices you want Security Cloud Control to manage must allow full inbound access from your SDC host on port 443 (or whichever port you have configured for your device management). This is configured using a management access control rule.

You must also ensure that the virtual machine on which the SDC is deployed has network connectivity to the management interface of the managed device.

Deploy a Secure Device Connector Using Security Cloud Control's VM Image

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. Adaptive Security Appliances (ASAs), FDM-managed devices, Firepower Management Centers (FMCs), and SSH and IOS devices, can all be onboarded to Security Cloud Control using an SDC.

The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices, and messages that need to be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control, sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control.

The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices. See Using Multiple SDCs on a Single Security Cloud Control Tenant, on page 35 for more information.

This procedure describes how to install an SDC in your network, using Security Cloud Control's VM image. This is the preferred, easiest, and most reliable way to create an SDC. If you need to create the SDC using a VM that you create, follow Deploy a Secure Device Connector On Your VM, on page 21.

Before you begin

Review these prerequisites before you deploy the SDC:

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the Secure Device Connector (SDC) and the Internet. If using a proxy server, disable inspection for traffic between the SDC and Security Cloud Control.
- The SDC must have full outbound access to the internet on TCP port 443, or the port you have configured for device management. The devices managed by Security Cloud Control must also allow inbound traffic from this port.
- Review Connect Security Cloud Control to your Managed Devices to ensure proper network access.
- Security Cloud Control supports installing its SDC VM OVF image using the vSphere web client or the ESXi web client.
- Security Cloud Control does not support installing the SDC VM OVF image using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Cent OS 7 guest operating system.
- System requirements for a VMware ESXi host with only one SDC:
  - VMware ESXi host needs 2 CPU.
  - VMware ESXi host needs a minimum of 2 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice.
- System requirements for a VM with an SDC and **a single** Secure Event Connector (SEC) for your tenant. (The SEC is a component used in About Security Analytics and Logging (SaaS) in Security Cloud Control).

  Each SEC that you add to the VMware ESXi host requires an additional 4 CPUs and an additional 8 GB of memory.

  Therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:
  - VMware ESXi host needs 6 CPU.
  - VMware ESXi host needs a minimum of 10 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice.
- The dockers IP must be in a different subnet than the SDC's IP range **and** the device IP range.
- Gather this information before you begin the installation:
  - Static IP address you want to use for your SDC.
  - Passwords for the `root` and `cdo` users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the SDC address is on.
  - The FQDN or IP address of your time server.
- The SDC virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

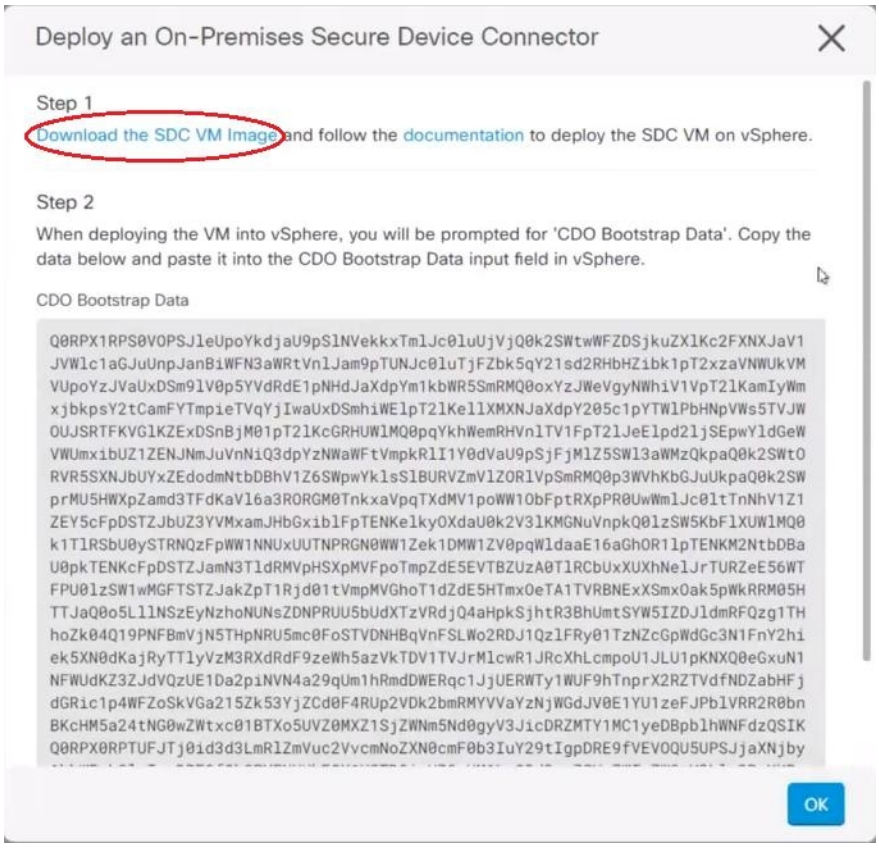
Procedure

Step 1 Log on to the Security Cloud Control Tenant you are creating the SDC for.

Step 2 In the left pane, click **Administration** > **Secure Connectors**.

Step 3 On the **Services** page, select the **Secure Connectors** tab, click the blue plus button, and select **Secure Device Connector**.

Step 4 In Step 1, click **Download the SDC VM image**. This opens in a separate tab.



Step 5 Extract all the files from the .zip file. They will look similar to these:

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

Step 6 Log on to your VMware server as an administrator using the vSphere Web Client.

Note Do not use the ESXi Web Client.

Step 7 Deploy the Secure Device Connector virtual machine from the OVF template by following the prompts.

Step 8 When the setup is complete, power on the SDC VM.

Step 9 Open the console for your new SDC VM.

Step 10 Login with the username "CDO". The default password is **adm123**.

Step 11 At the prompt, type `sudo sdc-onboard setup`.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

Step 12 When prompted for the password, enter `adm123`.

Step 13 Follow the prompts to create a new password for user `root`. Enter your password for the root user.

Step 14 Follow the prompts to create a new password for the Security Cloud Control user. Enter your password for the user

Step 15 When prompted with **Please choose the Security Cloud Control domain you connect to**, enter your Security Cloud Control domain information.

Step 16 Enter the following domain information of the SDC VM when prompted:

a) IP Address/CIDR
b) Gateway
c) DNS Server
d) NTP Server or FQDN
e) Docker Bridge

or press enter if a docker bridge is not applicable.

Step 17 When prompted with **Are these values correct? (y/n),** confirm your entries with **y.**

Step 18 Confirm your entries.

Step 19 When prompted with **Would you like to setup the SDC now? (y/n)**, enter `n`.

Step 20 The VM console automatically logs you out.

Step 21 Create an SSH connection to the SDC. Login as: CDO and enter your password.

Step 22 At the prompt, type `sudo sdc-onboard bootstrap`.

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

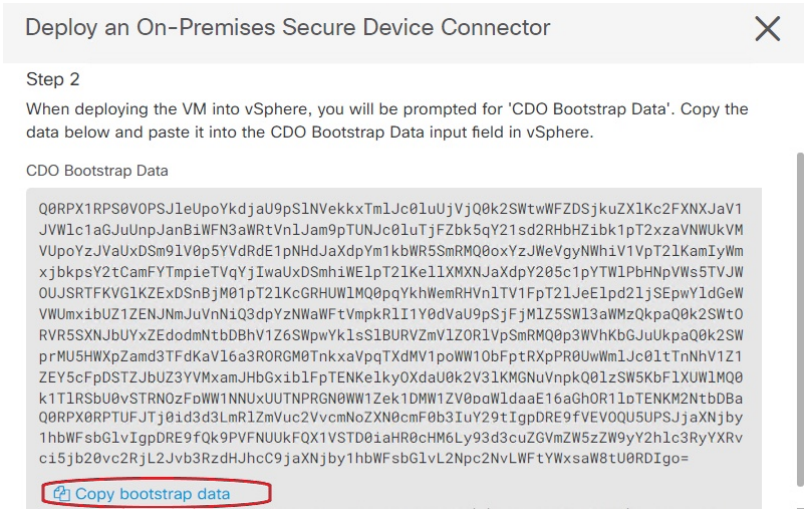
Step 23 When prompted with **[sudo] password**, enter the password you created in Step 14.

Step 24 When prompted with **Please copy the bootstrap data from the Secure Connector Page of Security Cloud Control**, follow this procedure:

a. Log into Security Cloud Control.

b. In the Actions pane, click **Deploy an On-Premises Secure Device Connector**.

c. Click **Copy the bootstrap data** in step 2 of the dialog box and paste into the SSH window.



Step 25 When prompted with **Do you want to update these setting? (y/n)**, enter `n`.

Step 26 Return to the Secure Device Connector page. Refresh the screen until you see the status of your new SDC change to **Active**.

Deploy a Secure Device Connector On Your VM

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. Adaptive Security Appliances (ASAs), FDM-managed devices, and Firepower Management Centers (FMCs) devices can all be onboarded to Security Cloud Control using device credentials.

The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices, and messages that need to be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control, sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control.

The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices. See Using Multiple SDCs on a Single Security Cloud Control Tenant, on page 35 for more information.

This procedure describes how to install an SDC in your network by using your own virtual machine image.

Note The preferred, easiest, and most reliable way to install an SDC is to download Security Cloud Control's SDC OVA image and install it. See Deploy a Secure Device Connector Using Security Cloud Control's VM Image, on page 17 for those instructions.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the SDC and the Internet.
- The SDC must have full outbound access to the Internet on TCP port 443 in order for it to communicate with Security Cloud Control.
- Devices that reach Security Cloud Control through the SDC must allow inbound access from the SDC on port 443.
- Review Connect Security Cloud Control to your Managed Devices for networking guidelines.
- VMware ESXi host installed with vCenter web client or ESXi web client.

Note We do not support installation using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Cent OS 7 guest operating system.
- System requirements for a VM with only an SDC:
  - VMware ESXi host needs 2 CPUs.
  - VMware ESXi host needs a minimum of 2 GB of memory.

- VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice. This value assumes you are using Logical Volume Management (LVM) with the partition so you can expand required disk space as needed.

- System requirements for a VM with an SDC and **a single** Secure Event Connector (SEC) for your tenant. (The SEC is a component used in About Security Analytics and Logging (SaaS) in Security Cloud Control).

  Each SEC you add to the VMware ESXi host requires an additional 4 CPUs and an additional 8 GB of memory.

  Therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:

  - VMware ESXi host needs 6 CPU.
  - VMware ESXi host needs a minimum of 10 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice.

- After you have updated the CPU and memory on the VM, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.
- Users performing this procedure should be comfortable working in a Linux environment and using the vi visual editor for editing files.
- If you are installing your on-premise SDC on a CentOS virtual machine, we recommend you install Yum security patches on a regular basis. Depending on your Yum configuration, to acquire Yum updates, you may need to open outbound access on port 80 as well as 443. You will also need to configure yum-cron or crontab to schedule the updates. Work with your security-operations team to determine if any security policies need to change to allow you to get the Yum updates.

Note **Before you get started**: Do not copy and paste the commands in the procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

Procedure

Step 1 Log on to the Security Cloud Control tenant you are creating the SDC for.

Step 2 In the left pane, click **Administration** > **Secure Connectors**.

Step 3 On the **Services** page, select the **Secure Connectors** tab, click the blue plus button, and select **Secure Device Connector**.

Step 4 Copy the bootstrap data in step 2 on the window to a notepad.

Step 5 Install a **CentOS 7 virtual machine** with at least the following RAM and disk space allotted to the SDC:

- 8GB of RAM
- 10GB disk space

Step 6 Once installed, configure basic networking such as specifying the IP address for the SDC, the subnet mask, and gateway.

Step 7 Configure a DNS (Domain Name Server) server.

Step 8 Configure a NTP (Network Time Protocol) server.

Step 9 Install an SSH server on CentOS for easy interaction with SDC's CLI.

Step 10 Run a Yum update and then install the packages: **open-vm-tools**, **nettools**, and **bind-utils**

```
[root@sdc-vm ~]# yum update -y
                [root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

Step 11 Install the AWS CLI package; see https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html.

Note Do not use the **--user** flag.

Step 12 Install the Docker CE packages; see https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce

Note Use the "Install using the repository" method.

Step 13 Start the Docker service and enable it to start on boot:

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

Step 14 Create two users: "CDO" and "sdc." The CDO user will be the one you log in to run administrative functions (so you don't need to use the root user directly), and the sdc user will be the user to run the SDC docker container.

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

Step 15 Set a password for the CDO user.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

Step 16 Add the CDO user to the "wheel" group to give it administrative (sudo) privileges.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

Step 17 When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

Step 18 If the /etc/docker/daemon.json file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

Note Make sure that the group name entered in the "group" key matches the group you found in the /etc/group file the previous step.

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
        }
        [root@sdc-vm ~]# systemctl restart docker
        [root@sdc-vm ~]#
```

Step 19 If you are currently using a vSphere console session, switch over to SSH and log in with the "CDO" user. Once logged in, change to the "sdc" user. When prompted for a password, enter the password for the "CDO" user.

```
[CDO@sdc-vm ~]$ sudo su sdc
              [sudo] password for cdo: <type password for cdo user>
              [sdc@sdc-vm ~]$
```

Step 20 Change directories to **/usr/local/CDO**.

Step 21 Create a new file called `bootstrapdata` and paste the bootstrap data from Step 2 of the **Deploy an On-Premises Secure Device Connector** wizard into this file. **Save** the file. You can use `vi` or `nano` to create the file.

Step 22 The bootstrap data comes encoded in base64. Decode it and export it to a file called `extractedbootstrapdata`

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/ CDO/bootstrapdata >
/usr/local/CDO/extractedbootstrapdata
             [sdc@sdc-vm ~]$
```

Run the cat command to view the decoded data. The command and decoded data should look similar to this:

```
[sdc@sdc-vm ~]$ cat /usr/local/ CDO/extractedbootstrapdata
              CDO_TOKEN="<token string>"
              CDO_DOMAIN="www.defenseorchestrator.com"
              CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

Step 23 Run the following command to export the sections of the decoded bootstrap data to environment variables.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
             [sdc@sdc-vm ~]$
```

Step 24 Download the bootstrap bundle from Security Cloud Control.

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
              100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
              [sdc@sdc-vm ~]$ ls -l /usr/local/ CDO/*SDC
              -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/CDO/tenant-name-SDC
```

Step 25 Extract the SDC tarball, and run the `bootstrap.sh` file to install the SDC package.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/CDO/tenant-name-SDC
              <snipped - extracted files>
              [sdc@sdc-vm ~]$
              [sdc@sdc-vm ~]$ /usr/local/ CDO/bootstrap/bootstrap.sh
              [2018-07-23 13:54:02] environment properly configured
              download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
              toolkit.sh
```

```
                common.sh
                [2018-07-23 13:54:04] startup new container
                Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
                sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
                ciscodefenseorchestrator/sdc_prod
                08d48e6f1cff: Pull complete
                ebbd10b629b1: Pull complete
                d14d580ef2ed: Pull complete
                45421d451ab8: Pull complete
                <snipped - downloads>
                no crontab for sdc
```

The SDC should now show "Active" in Security Cloud Control.

What to do next

-
- Return to Install a Secure Event Connector on an SDC Virtual Machine, on page 627 if you are installing a Secure Event Connector.
- Return to Installing an SEC Using a Security Cloud Control Image, if you are installing your **second or more** Secure Event Connectors on your tenant.

Deploy Secure Device Connector and Secure Event Connector on Ubuntu Virtual Machine

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. Adaptive Security Appliances (ASAs), FDM-managed devices, and Firepower Management Centers (FMCs) devices can all be onboarded to Security Cloud Control using device credentials.

The SDC monitors Security Cloud Control for commands that must be executed on your managed devices, and messages that must be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control, sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control.

The Secure Event Connector (SEC) forwards events from ASA and FTD to the Cisco cloud so that you can view them on the Event Logging page and investigate them with Secure Cloud Analytics, depending on your licensing.

After deploying the SDC, adding an SEC container becomes a simple task. The SEC service is designed to receive syslog messages from ASA, Cisco IOS and FDM-managed devices, and send them securely to the Cisco cloud. This allows eventing services like Security Cloud Control Analytics and Cisco XDR to store, augment, and analyze the log messages with ease.

You can execute the scripts that are provided on the CiscoDevNet site to install the SDC and SEC on Linux Ubuntu systems.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the SDCand the Internet.
- The SDC must have full outbound access to the Internet on TCP port 443.
- Review Connect Security Cloud Control to your Managed Devices for networking guidelines.
- VMware ESXi host that is installed with vCenter web client or ESXi web client.

Note We do not support installation using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Ubuntu operating system version 20.04 or above is installed on the virtual machine.

  SDC:

  - CPU: 2 Cores
  - RAM: Minimum of 2 GB

  SDC and SEC:

  - CPU: 4 Cores
  - RAM: Minimum of 8 GB

- The Ubuntu machine running the SDC must have network access to the management interfaces of the ASAs and Cisco IOS devices.

Procedure

Step 1 Log on to the Security Cloud Control tenant you are creating the SDC for.

Step 2 In the left pane, click **Administration** > **Secure Connectors**.

Step 3 On the **Services** page, select the **Secure Connectors** tab, click the  , and select **Secure Device Connector**.

Step 4 Copy the bootstrap data in step 2 on the window to a notepad.

Step 5 Open CiscoDevNet to Deploy SDC.

Step 6 Click **Code** and copy the URL in the **HTTPS** tab.

Step 7 On the Ubuntu system. press Ctrl+Alt+T to quickly open the terminal window.

Step 8 In the terminal, type **git** and paste the HTTPS URL copied earlier.

```
[sdc@vm]:~$ git https://github.com/CiscoDevNet/cdo-deploy-sdc.git
Resolving deltas: 100% (22/22). done.
```

Step 9 Go to the "cdo-deploy-sdc" directory.

```
[sdc@vm]:~$ cd cdo-deploy-sdc.
```

Step 10 Execute **ls -la** to see the files and scripts.

- **delete_sdc.sh**: Deletes SDC previously installed on your system.
- **deploy_sdc.sh**: Deploys SDC on your system.
- **install_docker.sh**: Deploys the recommended version of docker on your system.

Step 11 Run the script to install the docker.

```
[sdc@vm]:~/cdo-deploy-sdc$ ./install_docker.sh

Remove docker docker.io docker-compose docker-compose-v2 docker-doc podmand-docker {y/n] n
Active: active (running) since date time UTC; 32s ago
Adding the current user to the docker permmissions group
Done!
```

Step 12 Run the script to deploy SDC.

Enter **./deploy_sdc.sh** and paste the bootstrap data that is copied from the Security Cloud Control UI.

```
[sdc@vm]:~/cdo-deploy-sdc$ ./deploy_sdc.sh <bootstap data>.

If the docker container is up and running, the status of the SDC should go to 'Active' in
the Security Cloud Control Event Connectors panel.
```

The Secure Device Connector must now show "Active" in Security Cloud Control.

What to do next

-
- Go to Deploy Secure Event Connector on Ubuntu Virtual Machine, on page 636 to install a Secure Event Connector.

Deploy a Secure Device Connector to vSphere Using Terraform

Before you begin

This procedure details how you can use the Security Cloud Control SDC Terraform module for vSphere in conjunction with the Security Cloud Control Terraform Provider to deploy an SDC to your vSphere. Ensure you review the following prerequisites before attempting to perform this task procedure:

- You require a vSphere datacenter version 7 and above
- You require an admin account on the datacenter with permissions to do the following:
  - Create VMs
  - Create folders
  - Create content libraries
  - Upload files to content libraries
- Terraform knowledge

Procedure

Step 1 Create an API-only user in Security Cloud Control and copy the API token. To know how to create an API-only user, see Create API Only Users.

Step 2 Configure the Security Cloud Control Terraform provider in your Terraform repository by following the instructions in Security Cloud Control Terraform Provider.

Example:

```
terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = “<the CDO URL you use to access CDO>”
  api_token = “<the API Token generated in step 1>”
}
```

Step 3 Write Terraform code to create a `cdo_sdc` resource using the Security Cloud Control Terraform provider. See the Terraform registry for Security Cloud Control-sdc resource for more information.

Example:

```
Resource “cdo_sdc” “my-sdc” {
  name = “my-sdc-in-vsphere”
}
```

The `bootstrap_data` attribute of this resource is populated with the value of the Security Cloud Control bootstrap data and is provided to the `cdo_sdc` Terraform module in the next step.

Step 4 Write Terraform code to create the SDC in vSphere using Security Cloud Control_sdc Terraform module.

Example:

```
data "cdo_tenant" "current" {}

module "vsphere-cdo-sdc" {
  source               = "CiscoDevNet/cdo-sdc/vsphere"
  version              = "1.0.0"
  vsphere_username     = "<replace-with-username-with-admin-privileges>"
  vsphere_password     = "<super-secure-password>"
  vsphere_server       = "<replace-with-address-of-vsphere-server>"
  datacenter           = "<replace-with-datacenter-name>"
  resource_pool        = "<replace-with-resource-pool-name>"
  cdo_tenant_name      = data.cdo_tenant.current.human_readable_name
  datastore            = "<replace-with-name-of-datastore-to-deploy-vm-in>"
  network              = "<replace-with-name-of-network-to-deploy-vm-in>"
  host                 = "<replace-with-esxi-host-address>"
  allow_unverified_ssl = <boolean; set to true if your vsphere server does not have a valid
 SSL certificate>
  ip_address          = "<sdc-vm-ip-address; must be in the subnet of the assigned network
 for the VM>"
  gateway              = "<replace-with-network-gateway-address>"
  cdo_user_password    = "<replace-with-password-for-cdo-user-in-sdc-vm>"
  root_user_password   = "<replace-with-password-for-root-user-in-sdc-vm>"
```

```
  cdo_bootstrap_data    = cdo_sdc.sdc-in-vsphere.bootstrap_data
}
```

Note that the VM created has two users—a `root` user and a user called `cdo`—and the IP Address of the VM is configured statically. The `cdo_bootstrap_data` attribute is given the value of the `bootstrap_data` attribute generated when the `cdo_sdc` resource is created.

Step 5 Plan and apply your Terraform using `terraform plan` and `terraform apply`, as you would normally.

See the Security Cloud Control Automation Repository in the CiscoDevNet for a complete example.

If your SDC stays in the onboarding state, connect to the vSphere VM using remote console, log in as the CDO user, and execute the following command:

```
sudo su
/opt/cdo/configure.sh startup
```

Note The Security Cloud Control Terraform modules are published as Open Source Software under the Apache 2.0 license. You can file issues on GitHub if you require support.

Deploy a Secure Device Connector on an AWS VPC Using a Terraform Module

Before you begin

Review these prerequisites before attempting to deploy an SDC on your AWS VPC:

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the SDC and the Internet. If using a proxy server, disable inspection for traffic between the Secure Device Connector (SDC) andSecurity Cloud Control.
- Review Connect Security Cloud Control to your Managed Devices to ensure proper network access.
- You require an AWS account, an AWS VPC with at least one subnet, and an AWS Route53-hosted zone.
- Ensure you have the Security Cloud Control bootstrap data, your AWS VPC ID, and its subnet ID handy.
- Ensure that the private subnet to which you deploy the SDC has a NAT gateway attached.
- Open traffic on the port on which your firewall management HTTP interface is running, from your firewalls to the Elastic IP attached to the NAT gateway.

Procedure

Step 1 Add the following lines of code in your Terraform file; make sure you manually enter inputs for variables:

```
module "example-sdc" {
  source              =
"git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env                 = "example-env-ci"
  instance_name       = "example-instance-name"
  instance_size       = "r5a.xlarge"
```

```
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id             = <replace-with-vpc-id>
  subnet_id          = <replace-with-private-subnet-id>
}
```

See the Secure Device Connector Terraform module for a list of input variables and descriptions.

Step 2 Register `instance_id` as an output in your Terraform code:

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

You can use the `instance_id` to connect to the SDC instance for troubleshooting using the AWS Systems Manager Session Manager (SSM). See Outputs in the Secure Device Connector Terraform module for a list of available outputs.

What to do next

For any troubleshooting of your SDC, you need to connect to the SDC instance using AWS SSM. See AWS Systems Manager Session Manager to know more about how to connect to your instance. Note that the ports to connect to the SDC instance using SSH are not exposed because of security reasons.

Note The Security Cloud Control Terraform modules are published as Open Source Software under the Apache 2.0 license. You can file issues on GitHub if you require support.

Configure a Secure Device Connector to Use Proxy

Using a proxy server can enhance security by acting as an intermediary that filters outbound traffic. It prevents direct exposure of your network devices to the internet and reduces the risk of attacks. A proxy server can be integrated with the Secure Device Connector (SDC) for all outbound communications from the SDC to Security Cloud Control. This procedure focuses on modifying the Docker container configuration specific to the SDC, not the host Linux OS settings.

Note The changes affect only the SDC's Docker container. Configure the proxy settings for the host Linux system according to your organization's standard procedures for Linux servers.

Before you begin

- Familiarity with the Linux command-line interface (CLI) is required.
- We recommend creating a backup of your config.json file before editing it.

Procedure

Step 1 Access the SDC using SSH and switch to the SDC user using this command:

```
$ sudo su - sdc
```

Step 2 Navigate to the configuration file at `/usr/local/cdo/data/<your_sdc_name>/data/config.json`.

Step 3 Insert the JSON key-value pair into the config.json file.

Replace proxy with your proxy server's IP address or FQDN, and port with the proxy server's listening port.

```
"awsProxy":"https://proxy:port"
```

Step 4 Save the changes and restart the SDC container. You can do this by either restarting the Docker container directly or by rebooting the virtual machine hosting the SDC.

a) To restart the Docker container, first identify the SDC container ID using this command:

```
[sdc@localhost cdo] $ docker ps
```

b) Restart the container using this command:

```
[sdc@localhost cdo] $ docker restart <container_id>
```

where *<container_id>* is the ID of the SDC container.

Step 5 Check the status using this command, and ensure that the SDC container has restarted successfully and is operational:

```
[sdc@localhost cdo] $ docker ps | grep sdc
```

Verify that the proxy settings are correct in the logs/lar.log file using this command:

```
[sdc@localhost cdo] $ less /usr/local/cdo/data/<your_sdc_name>/logs/lar.log
```

The SDC is successfully configured to communicate using the proxy server.

Change the IP Address of a Secure Device Connector

Before you begin

- You must be an admin to perform this task.
- The SDC must have full outbound access to the Internet on TCP port 443, or the port you have configured for device management.

Note You will not be required to re-onboard any devices to Security Cloud Control after changing the SDC's IP address.

Procedure

Step 1 Create an SSH connection to your SDC or open your virtual machine's console, and log in as the Security Cloud Control user.

Step 2 If you wish to view your SDC VM's network interface configuration information before changing the IP address, use the `ifconfig` command.

```
[cdo@localhost ~]$ ifconfig
```

Step 3 To change the IP address of the interface, type `sudo sdc-onboard setup` command.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

Step 4 Enter your password at the prompt.

```
[sudo] password for Security Cloud Control:
```

Step 5 Type `n` at the prompt for resetting the root and Security Cloud Control passwords.

```
Would you like to reset the root and cdo passwords? (y/n):
```

Step 6 Type `y` at the prompt for reconfiguring the network.

```
Would you like to re-configure the network? (y/n):
```

Step 7 Enter the new IP address you wish to assign to your SDC and the other domain information of the SDC VM when prompted:

a) IP Address
b) Gateway
c) DNS Server
d) NTP Server or FQDN

   or press enter if an NTP server or FQDN is not applicable.

e) Docker Bridge

   or press enter if a docker bridge is not applicable.

Step 8 Confirm your entries with `y` when prompted for the correctness of the values.

```
Are these values correct? (y/n):
```

Note Make sure your values are accurate before typing `y`, because your SSH connection to the old IP address will be lost after this command.

Step 9 Create an SSH connection using the new IP address you assigned to your SDC and log in.

Step 10 You can run the connectivity status test command to ensure that your SDC is up and running.

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

All the checks must say `[ OK ]` in green.

Note If you are performing this procedure in the VM's console, once you confirm the values are correct, the connectivity status test is automatically run and the status shown.

Step 11 You can also check your SDC's connectivity through the Security Cloud Control user interface. To do that, open the Security Cloud Control application and navigate to **Administration** > **Secure Connectors** page.

Step 12 Refresh the page once and select the secure connector whose IP address you changed.

Step 13 On the **Actions** pane, click **Request Heartbeat**.

You should see the **Hearbeat requested successfully** message, and the **Last Heartbeat** should display the current date and time.

Important The IP address change you made gets reflected on the SDC's **Details** pane only after 3:00 AM GMT.

See Deploy a Secure Device Connector On Your VM, on page 21 for information on deploying an SDC on your VM.

Remove a Secure Device Connector

Warning This procedure deletes your Secure Device Connector (SDC). It is not reversible. After taking this action, you will not be able to manage the devices connected to that SDC until you install a new SDC and reconnect your devices. Reconnecting your devices may requires you to re-enter the administrator credentials for each device you need to reconnect.

To remove the SDC from your tenant, follow this procedure:

Procedure

Step 1 Remove any devices connected to the SDC you want to delete.

- **a.** See Security Cloud Control Devices that Use the Same SDC to identify all the devices used by the SDC.
- **b.** In the **Inventory** page, select all the devices you identified.
- **c.** In the Device Actions pane, click **Remove** and click **OK** to confirm your action.

Step 2 In the left pane, click **Administration** > **Secure Connectors**.

Step 3 On the **Services** page with the **Secure Connectors** tab selected, click the blue plus button and select **Secure Device Connector**.

Step 4 In the Secure Connectors table, select the SDC you want to remove. Its device count should now be zero.

Step 5 In the Actions pane, click **Remove**. You receive this warning:

Warning You are about to delete <sdc_name>. Deleting the SDC is not reversible. Deleting the SDC will require you to create and onboard a new SDC before you can onboard, or re-onboard, your devices.

Because you currently have onboarded devices, removing the SDC will require you to reconnect those devices and provide credentials again after setting up a new SDC.

- If you have any questions or concerns, click **Cancel** and contact Security Cloud Control support.
- If you wish to proceed, enter <sdc_name> in the text box below and click **OK**.

Step 6 In the confirmation dialog box, if you wish to proceed, enter your SDC's name as it is stated in the warning message.

Step 7 Click **OK** to confirm the SDC removal.

Move an ASA from one SDC to Another

Security Cloud Control Using Multiple SDCs on a Single Security Cloud Control Tenant. You can move a managed ASA from one SDC to another using this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **ASA** tab.

Step 3 Select the ASA or ASAs you want to move to a different SDC.

Step 4 In the **Device Actions** pane, click **Update Credentials**.

Step 5 Click the Secure Device Connector button and select the SDC you want to move the device to.

Step 6 Enter the administrator username and password Security Cloud Control uses to log into the device and click **Update**. Unless they were changed, the administrator username and password are the same credentials you used to onboard the ASA. You do not have to deploy these changes to the device.

Note If all the ASAs use the same credentials, you can move ASAs in bulk from one SDC to another. If the ASAs have different credentials, you have to move them from one SDC to another one at a time.

Rename a Secure Device Connector

Procedure

Step 1 In the left pane, choose **Tools & Services** > **Secure Connectors**.

Step 2 Select the SDC you want to rename.

Step 3 In the Details pane, click the edit icon next to the name of the SDC.

Step 4 Rename the SDC.

This new name will appear wherever the SDC name appears in the Security Cloud Control interface including the Secure Device Connectors filter of the **Inventory** pane.

Update your Secure Device Connector

Use this procedure as a troubleshooting tool. Ordinarily, the SDC is updated automatically and you should not have to use this procedure. However, if the time configuration on the VM is incorrect, the SDC cannot establish a connection to AWS to receive the updates. This procedure will initiate an update of the SDC and should resolve errors due to time synchronization problems.

Procedure

Step 1 Connect to your SDC. You can connect using SSH or use the console view in your VMware Hypervisor.)

Step 2 Log in to the SDC as the **cdo** user.

Step 3 Switch to the SDC user to update the SDC docker container:

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

Step 4 Upgrade the SDC toolkit:

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

Step 5 Upgrade the SDC:

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

Note **Recommended updates and maintenance on the SDC Virtual Machine**

Ensure that you monitor and apply updates to the SDC VM running on Ubuntu Linux following your organisation's internal IT security and patch management policies. We highly recommend regularly reviewing and applying relevant security patches to ensure that the SDC VM remains secure and functions optimally within your network environment.

Using Multiple SDCs on a Single Security Cloud Control Tenant

Deploying more than one SDC for your tenant allows you to manage more devices without experiencing performance degradation. The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files.

You can install an unlimited number of SDCs on a tenant. Each SDC could manage one network segment. These SDCs would connect the devices in those network segments to the same Security Cloud Control tenant. Without multiple SDCs, you would need to manage the devices in isolated network segments with different Security Cloud Control tenants.

The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC. Deploy a Secure Device Connector Using Security Cloud Control's VM Image or you can Deploy a Secure Device Connector On Your VM. The initial SDC for your tenant incorporates the name of your tenant and the number 1. Each additional SDC is numbered in order.

Security Cloud Control Devices that Use the Same SDC

Follow this procedure to identify all the devices that connect to Security Cloud Control using the same SDC:

Procedure

Step 1 In the left pane, **Security Devices**.

Step 2 Click the **Devices** tab to locate the device.

Step 3 Click the appropriate device type tab.

Step 4 If there is any filter criteria already specified, click the **clear** button at the top of the Inventory table to show all the devices and services you manage with Security Cloud Control.

Step 5 Click the filter button to expand the Filters menu.

Step 6 In the Secure Device Connectors section of the filter, check the name of the SDC(s) you're interested in. The Inventory table displays only the devices that connect to Security Cloud Control through the SDC you checked in the filter.

Step 7 (Optional) Check additional filters in the filter menu to refine your search further.

Step 8 (Optional) When you're done, click the **clear** button at the top of the Inventory table to show all devices and services you manage with Security Cloud Control.

Open Source and Third-Party License in SDC

==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

This package, "amqplib", is licensed under the MIT License. A copy maybe found in the file LICENSE-MIT in this directory, or downloaded from

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT

OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** bluebird ***

The MIT License (MIT)

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the 'Software'), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** command-line-args ***

The MIT License (MIT)

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** ip ***

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

Permission is hereby granted, free of charge,to any person obtaining a copy of this software andassociated documentation files (the "Software"), todeal in the Software without restriction, includingwithout limitation the rights to use, copy, modify,merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whomthe Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission noticeshall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIESOF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FORANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stable-stringify ***

This software is released under the MIT license:

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS ORCOPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHERIN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR INCONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/>

Based on Underscore.js, copyright Jeremy Ashkenas,

DocumentCloud and Investigative Reporters & Editors<http://underscorejs.org/>

This software consists of voluntary contributions made by manyindividuals. For exact contribution history, see the revision historyavailable at https://github.com/lodash/lodash

The following license applies to all parts of this software except as

documented below:

====

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Samplecode is defined as all source code displayed within the prose of thedocumentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externallymaintained libraries used by this software which have their ownlicenses; we recommend you read them, as their terms may differ from theterms above.

==========

*** log4js ***

Copyright 2015 Gareth Jones (with contributions from many other people)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions andlimitations under the License.

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

This project is free software released under the MIT/X11 license:

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including

without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

*** Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.**

*** Redistributions in binary form must reproduce the above copyrightnotice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.**

*** Neither the name of Digital Bazaar, Inc. nor thenames of its contributors may be used to endorse or promote productsderived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" ANDANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AREDISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANYDIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED ANDON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THISSOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

*** request ***

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution

incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT License - http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Devices, Software, and Hardware Supported by Security Cloud Control

Security Cloud Control is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms. Security Cloud Control centrally manages policy and configuration across:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Secure Firewall Management Center, on-premises
- Cisco Meraki MX
- Cisco IOS devices
- Cisco Umbrella
- AWS Security Groups

The documentation describes devices, software, and hardware Security Cloud Control supports. It does not point out software and devices that Security Cloud Control does not support. If we do not explicitly claim support for a software version or a device type, then we do not support it.

Cisco Secure Firewall ASA

Cisco Adaptive Security Appliance (ASA) is a security device integrating firewall, VPN, and intrusion prevention capabilities. It protects networks from unauthorized access, cyber threats, and data breaches, offering robust security services in a single platform. Security Cloud Control supports the management of ASA devices, offering features to streamline configuration management and ensure regulatory compliance across the network infrastructure.

Cisco Secure Firewall Threat Defense

Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It offers comprehensive security functions, including intrusion prevention, application control, URL filtering, advanced malware protection, and so on. An FTD can be deployed on ASA hardware appliances, and Cisco firewall hardware appliances, and in virtual environments. Managing threat defense devices is possible through various management interfaces, such as Cisco Firewall Management Center, Security Cloud Control, and Firewall Device Manager.

For more information on software and hardware compatibility, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Firewall Device Manager is a web-based management interface explicitly designed for threat defense device management. It provides a simplified approach for configuring and monitoring threat defense devices, making it ideal for smaller-scale deployments or organizations preferring an intuitive interface.

FDM offers basic configuration capabilities for network settings, access control policies, NAT rules, VPN configuration, monitoring, and basic troubleshooting. Typically accessed through a web browser, FDM is directly available on the FTD device, eliminating the need for additional management servers or appliances.

Cisco Secure Firewall Management Center

Security Cloud Control simplifies the management of on-premises Firewall Management Center by establishing a secure integration, discovering device inventories, and enabling centralized policy management. Security policies such as firewall rules, VPN settings, and intrusion prevention policies can be efficiently managed and deployed across all devices under FMC.

Cisco Meraki MX

The Meraki MX appliance is an enterprise-grade security and SD-WAN next-generation firewall appliance, designed for decentralized deployments. Security Cloud Control supports managing layer 3 network rules on Meraki MX devices. When you onboard a Meraki device to Security Cloud Control, it communicates with the Meraki dashboard to manage that device. Security Cloud Control securely transfers configuration requests to the Meraki dashboard, which then applies the new configuration to the device. Key features of Security Cloud Control's support for Cisco Meraki MX include centralized policy management, backup and restore, monitoring and reporting, compliance checking, and automation capabilities.

Cisco IOS Devices

Cisco IOS can manage and control network functions, including routing, switching, and other networking protocols. It offers a set of features and commands to configure and maintain Cisco network devices, enabling efficient communication and management within networks of varying sizes and complexities.

Cisco Umbrella

Security Cloud Control manages Cisco Umbrella through integrations such as the Umbrella ASA Integration, which allows administrators to include their Cisco Adaptive Security Appliance (ASA) within their Umbrella

configuration using per-interface policies. This integration enables the ASA to redirect DNS queries to Umbrella, enhancing network security by leveraging Umbrella's DNS security, web filtering, and threat intelligence capabilities.

AWS Security Groups

Security Cloud Control offers a simplified management interface for Amazon Web Services (AWS) Virtual Private Clouds (VPCs). Key features include monitoring AWS Site-to-Site VPN connections, tracking changes to AWS devices, and viewing AWS Site-to-Site VPN tunnels.

Secure Firewall Threat Defense Device Support Specifics

Secure Firewall Threat Defense is Cisco's next generation firewall. It can be installed on a variety of hardware and virtual platforms; see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Threat Defense with Secure Firewall Device Manager

You can add Security Cloud Control managment to threat defense Version 6.4+ with device manager. However, this option is only available upon request for those who already have device manager support enabled on their tenant. See:

- Open a Support Ticket with TAC, on page 781 to request this option.
- Managing FDM-Managed Devices with Cisco Security Cloud Control to review the supported features.
- Onboard a Threat Defense Device for a full discussion of onboarding prerequisites and requirements.
- Guidelines and Limitations for Firepower Interface Configuration for Security Cloud Control limitations.

Snort

Snort 3 is the default inspection engine for threat defense starting in threat defense Version 6.7 (with device manager) and Version 7.0 (with management center).

Important If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

Browsers Supported in Security Cloud Control

Security Cloud Control supports the latest version of these browsers:

- Google Chrome
- Mozilla Firefox

Security Cloud Control Platform Maintenance Schedule

Security Cloud Control updates its platform every week with new features and quality improvements. Updates are made during a 3 hour period according to this schedule:

Day of the Week	Time of Day (24-hour time, UTC)
Thursday	09:00 UTC - 12:00 UTC

During this maintenance period, you can still access your tenant and if you have a cloud-delivered Firewall Management Center or Multicloud Defense Controller, you can access those portals as well. Additionally, the devices you have onboarded to Security Cloud Control continue to enforce their security policies.

Note

- We advise against using Security Cloud Control to deploy configuration changes on the devices it manages during maintenance periods.
- If there is any issue that stops Security Cloud Control from communicating, we address that failure on all affected tenants as quickly as possible, even if it is outside the maintenance window.

Cloud-delivered Firewall Management Center Maintenance Schedule

Customers who have a cloud-delivered Firewall Management Center deployed on their tenant are notified approximately 1 week before Security Cloud Control updates the cloud-delivered Firewall Management Center environment. Super Admin and Admin users of the tenant are notified by email. Security Cloud Control also displays a banner on its home page notifying all users of upcoming updates.

Note

- We advise you not to use cloud-delivered Firewall Management Center to deploy configuration changes on the devices it manages during maintenance periods.
- If there is any issue that stops Security Cloud Control or cloud-delivered Firewall Management Center from communicating, that failure is addressed on all affected tenants as quickly as possible, even if it is outside the maintenance window.

Manage a Security Cloud Control Tenant

Security Cloud Control gives you the ability to customize certain aspects of your tenant, users, and notification preferences. Review the following settings available for customized configuration:

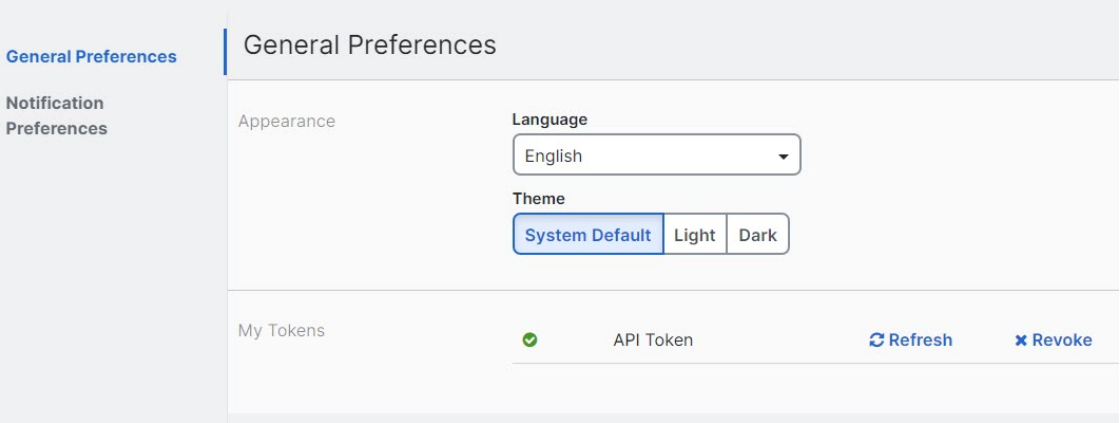
General Settings

See the following topics regarding general Security Cloud Control Settings:

- General Preferences, on page 49
- For **My Tokens**, see API Tokens, on page 62
- For **Tenant Settings**, see:
  - Enable Change Request Tracking, on page 50
  - Prevent Cisco Support from Viewing your Tenant, on page 50
  - Enable the Option to Auto-accept Device Changes, on page 51
  - Enable the Option to Schedule Automatic Deployments, on page 51
  - Default Conflict Detection Interval, on page 51
  - Web Analytics, on page 52
  - Configure a Default Recurring Backup Schedule, on page 52
  - Tenant ID, on page 53
  - Tenant Name, on page 53

General Preferences

Select the desired language and theme for the Security Cloud Control UI to display in. This selection only affects the user who makes this change.



Change the Security Cloud Control Web Interface Appearance

You can change the way the web interface appears.

Procedure

Step 1 From the drop-down list under your username, choose **Preferences**.

Step 2 In the **General Preferences** area, select a **Theme**:

- **Light**
- **Dark**

My Tokens

See API Tokens for more information.

Tenant Settings

Enable Change Request Tracking

Enabling change request tracking affects all users of your tenant. To enable Change Request Tracking, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the slider under **Change Request Tracking**.

Once confirmed, you see the Change Request toolbar appear in the lower left corner of the interface and the Change Request drop-down menu in the Change Log.

Prevent Cisco Support from Viewing your Tenant

Cisco support will associate its users with your tenant to resolve support tickets or proactively fix issues that affect more than one customer. However, if you prefer, you can prevent Cisco support from accessing your tenant by changing your account settings. To do so, slide the toggle button under **Prevent Cisco support from viewing this tenant** to show a green check mark.

To prevent Cisco support from viewing your tenant, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the slider under **Prevent Cisco support from viewing this tenant**.

Enable the Option to Auto-accept Device Changes

Enabling auto-accept for device changes allows Security Cloud Control to automatically accept any changes made directly on the device. If you leave this option disabled, or disable it at a later time, you are required to review each device conflict before you can accept it.

To enable auto-accept for device changes, follow this procedure:

Procedure

Step 1 In the left pane, **Administration** > **General Settings**.

Step 2 Click the slider under **Enable the option to auto-accept device changes**.

Default Conflict Detection Interval

This interval determines how often Security Cloud Control polls onboarded devices for changes. This selection affects all devices managed with this tenant, and can be changed at any time.

Note This selection can be overridden via the **Conflict Detection** option available from the **Inventory** page after you have selected one or multiple devices.

To configure this option and select a new interval for conflict detection, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the drop-down menu for **Default Conflict Detection Interval** and select a time value.

Enable the Option to Schedule Automatic Deployments

Enabling the option to schedule automatic deployments allows you to schedule future deployments at a date and time when it is convenient. Once enabled, you can schedule a single or a recurring automatic deployment. To schedule an automatic deployment, see Schedule an Automatic Deployment.

Note that changes made on Security Cloud Control for a device are not automatically deployed to the device if it has pending changes of its own  . If a device is not in the **Synced** state, such as **Conflict Detected** or **Not Synced**, scheduled deployments are not executed. The jobs page lists any instance where a scheduled deployment fails.

If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

Important If you use Security Cloud Control to create more than one scheduled deployment for a device, the new deployment overwrites the existing deployment. If you create more than one scheduled deployment a device using API, you **must** delete the existing deployment prior to schedule the new deployment.

To enable the option to schedule automatic deployments, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the slider under **Enable the option to schedule automatic deployments**.

Web Analytics

Web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted.

Web analytics is enabled by default. To disable web analytics, or to enable in the future, follow this procedure:

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Click the toggle under **Web Analytics**.

Configure a Default Recurring Backup Schedule

To make backup schedules across your devices consistent, use this setting to configure your own default recurring backup schedule. When you schedule a backup for a particular device, you can use the default settings or change them. Changing the default recurring backup schedule does not change any existing scheduled backups or recurring backup schedules.

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 In the Tenant Settings area, find the **Default Recurring Backup Schedule** section, and in **Frequency** field select daily, weekly, or monthly backup.

Step 3 Select the time of day, in 24-hour time, you want the backup to occur. Note that you schedule the time in Coordinated Universal Time (UTC).

- For weekly backups: Check the days of the week on which you want the backup to occur.

- For monthly backups: Click in the **Days of Month** field and add whichever days of the month you want to the schedule the backup. Note: If you enter day 31 but a month doesn't have 31 days in it, the backup will not take place. Give the scheduled backup time a name and a description.

Step 4 Click **Save**.

See Configure a Recurring Backup Schedule for a Single FDM-Managed Device for additional information.

Tenant ID

Your tenant ID identifies your tenant. This information will be helpful if you need to contact the Cisco Technical Assistance Center (TAC).

Tenant Name

Your tenant name also identifies your tenant. Note that the tenant name is not the organization name. This information will be helpful if you need to contact the Cisco Technical Assistance Center (TAC).

Security Cloud Control Platform Navigator

The platform navigator is a nine-block applications cross-launcher () that appears on the top right corner of Security Cloud Control. You can readily cross-launch to the following Cisco networking and security applications:

Networking Applications

- **Catalyst**—Cisco Catalyst products include a wide variety of network switches, wireless controllers, wireless access points, and edge platforms and routers, supporting enterprise-class business needs to heavy-duty and rugged networking environments.
- **Intersight**—Cisco Intersight is a cloud operations platform that consists of optional, modular capabilities of advanced infrastructure, workload optimization, and Kubernetes services. Cisco Intersight infrastructure services include the deployment, monitoring, management, and support of your physical and virtual infrastructure. It supports Cisco Unified Computing System (Cisco UCS) and Cisco HyperFlex hyperconverged infrastructure (HCI), and other third-party Intersight-connected targets.
- **IoT Operations Dashboard**—Cisco IoT Operations Dashboard is a cloud-based IoT services platform that empowers operations teams to securely connect, maintain, and gain insights from industrial networking devices and connected industrial assets at massive scale. With one comprehensive view of all their connected industrial assets, operation teams can uncover valuable insights that help them streamline operations and drive business continuity.
- **Meraki**—Cisco Meraki is an IT and IoT cloud-managed platform that provides a centralized management platform for Cisco Meraki devices.
- **Spaces**—Cisco Spaces is a cloud-based location services platform through which organizations can gain insights into how people and things move throughout their physical spaces. With these insights, they can deliver contextual engagements that are valuable and relevant. Besides looking at where people go, organizations can also drive operational efficiencies by monitoring the location, movement, and utilization of assets.

- **ThousandEyes**—Cisco ThousandEyes is a cloud service suite that helps monitor and measure the availability and performance of web applications, services, and networks. It provides end-to-end visibility from any user to any application over any network, enabling enterprises to swiftly get to the source of issues, resolve them faster, and manage performance effectively.
- **Workflows**—Cisco Workflows is a cloud-hosted automation application that is part of the larger Cisco Networking Cloud vision. Workflows provides an entitlement to cross-domain automation capabilities to current Cisco customers by streamlining repetitive and error-prone tasks across both Cisco and third-party applications through custom and premade automation templates and a plethora of adapter options, both provided by Cisco and build your own, to reach targets in the cloud or on-premises.

Security Applications

- **Duo Security**—Cisco Duo is a user-centric zero-trust security platform with two-factor authentication to protect access to sensitive data for all users, devices, and applications. It offers features such as adaptive policies, single sign-on (SSO), and advanced endpoint visibility, making it a comprehensive solution for securing remote access and maintaining business continuity.
- **Secure Access**—Cisco Secure Access simplifies IT operations through a single, cloud-managed console, unified client, centralized policy creation, and aggregated reporting. Extensive security capabilities converged in one solution (ZTNA, SWG, CASB, FWaaS, DNS security, RBI and more) mitigate security risk by applying zero trust principles and enforcing granular security policies. Market leading Talos threat intelligence fuels unmatched threat blocking to mitigate risk and speed investigations.
- **Secure Endpoint**—Cisco Secure Endpoint, formerly known as Cisco AMP for Endpoints, is a cloud-managed endpoint security solution designed to prevent breaches and rapidly detect, contain, and remediate threats. It is an instant check of your files against a cloud-based scanner with advanced tracking features that enable security analysts to determine and isolate initial sources of outbreaks, and it provides a retrospective quarantine of files that are discovered to be malicious.
- **Cisco Security Provisioning and Administration**—Cisco Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud. Security Cloud Control administrators can create new Security Cloud enterprises, manage users in an enterprise, claim domains, and integrate their organization's SSO identity provider, among other tasks.
- **XDR**—Cisco Extended Detection and Response (XDR) is a cloud-based solution designed to simplify security operations and empower security teams to detect, prioritize, and respond to sophisticated threats. By integrating both Cisco and third-party security solutions into a unified platform, Cisco XDR offers a comprehensive approach to threat management. Integrated with the threat intelligence provided by Talos, Cisco XDR enriches incident data with additional context and asset insights, reducing false positives and enhancing overall threat detection, response, and forensic capabilities.

View Security Cloud Control Notifications

Click the notifications icon  to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The selections that you make in the **Notification Settings** page impact the types of notifications displayed in Security Cloud Control. Continue reading for more information.

This drop-down page is grouped into three tabs: Overview, All, and Dismissed.

Overview Tab

The **Overview** tab displays a combination of the most recent high-prioroty alerts and events that you are subscribed to. High prioroty events are the following:

- Deployment Failed
- Backup Failed
- Upgrade Failed
- Migrate FTD to cdFMC Failed
- Device went offline
- Device HA state changed
- Device certificates expiring

You can configure which alerts you want to receive by clicking the Notification Settings in the Notifications window or by selecting **UserID** > **User Preferences** page. The User ID button in the upper right corner of the dashboard.

All Tab

The **All** tab displays all notifications regardless of their prioroty ranking, including email subscription notifications and all of the items listed as high priority.

Dismissed Tab

The **Dismissed** tab displays notifications you have dismissed. You can dsimiss individual notifications by clicking the "**x**" of the notification.

Opting to **Dismiss** notifications from the drop-down menu dismisses notifications from **both** the "Overview" and "All" tabs. They will remain in the **Dismiss** tab for 30 days, after which they will be removed from Security Cloud Control.

Search Notifications

When viewing the notifications drop-down window, for any of the tabs mentioned above, you can use the search bar at the top of the drop-down to query for key words or alerts.

User Notification Preferences

Notifications are generated by Security Cloud Control whenever a device associated with your tenant experiences a specific event, such as whenever a device associated with your tenant experiences a specific action, a device certificate is expiring or has expired, or a background log search starts, finishes or fails. The following notifications are enabled by default and displayed for every user that is affiliated with the tenant regardless of the user role. You can modify your personal notification preference to only show alerts you are interested in. Note that these preference are yours only and do not affect other users associated with the tenant.

Note Changes made to the notifications listed below are automatically updated in real time and do not require deployment.

View your personal preferences in the **Username ID** > **Preferences** > **Notification Preferences** page. Your Username ID is always located in the upper right corner of Security Cloud Control across all pages. From this page you can configure the following "**Notify Me in Security Cloud Control When**" alerts.

Send Alerts for Device Workflows

- **Deployments** - This action does not include integration instances for SSH or IOS devices.
- **Backups** - This action is only applicable for FDM-managed devices.
- **Upgrades** - This action is only applicable for ASA and FDM-managed devices.
- **Migrate threat defense to cloud** - This action is applicable when changing the threat defense device manager from Management Center to Security Cloud Control.

Send Alerts for Device Events

- **Went offline** - This action applies to all devices associated with your tenant.
- **Back online** - This action applies to all the devices associated with your tenant.
- **Conflict detected** - This action applies to all the devices associated with your tenant.
- **HA state changed** - This action indicates the device within an HA or failover pair, the current state, and the state it changed from. This action applies to all HA and failover configurations associated with your tenant.
- **Site-to-Site session disconnected** - This action applies to all site-to-site VPN configurations configured in your tenant.

Send Alerts for Background Log Search

- **Search started** - Receive a notification when a search starts. This applies to both immediate and scheduled searches.
- **Search completed** - Receive a notification when a search ends. This applies to both immediate and scheduled searches.
- **Search failed** - Receive a notification when a search fails. This applies to both immediate and scheduled searches. Check the parameters or the query and try again.

Opt Out of Notification Preferences

By default, all events are enabled and generate notifications. To opt out of notifications generated by the events mentioned above, you must manually **uncheck** the notification types. Note that you must click **Save** to confirm any changes.

Email Alerts

Enable the **Email Alerts** toggle to receive any of the alerts mentioned above. Check which alerts you would like to receive by email and click the **Save** button. By default, the **Use Security Cloud Control notification settings above** is checked. This means that you will receive email alerts on all of the same notifications and events as you have checked in the "Send Alerts When..." sections mentioned on this page.

If you only want **some** of the events or alerts mentioned above forwarded to your email, uncheck the **Use Security Cloud Control notification settings above"**. This action generates an additional location to modify and personalize the available alerts. This may help reduce redundancy.

Tenant Notification Settings

From the navigation bar to the left, click **Settings** > **Notification Settings**.

All users associated with your tenant will automatically receive these alerts. In addition, some or all of these alerts can be forwarded to specific emails or services.

Note You must have an **Super Admin** user role to change these settings. See User Roles in Security Cloud Control for more information.

Email Subscribers

Add or modify the emails that receive alerts from your Security Cloud Control tenant. See Enable Email Subscribers, on page 57 for more information.

Service Integrations

Enable Incoming Webhooks on your messaging app and receive Security Cloud Control notifications directly to your app dashboard. See Enable Service Integrations for Security Cloud Control Notifications for more information.

Enable Email Subscribers

An email notification from Security Cloud Control denotes the type of action and the affected devices. For further information about the current state of your devices and the content of the action, we recommend logging into Security Cloud Control and examining the Manage Change Logs in Security Cloud Control of the affected devices.

Warning Be sure to enter the correct email if you are adding a mailer. Security Cloud Control does not check email addresses against known users associated with your tenant.

Add an Email Subscription

Before you begin

You must be an **Admin** to view the email subscription list, and a **SuperAdmin** to add, remove, or edit email subscriptions.

Procedure

Step 1 In the left pane, click **Administration** > **Notification Settings**.

Step 2 Click the + icon in the upper right corner of the page.

Step 3 Enter a valid email address in the text field.

Step 4 Check and uncheck the appropriate checkboxes for events and alerts you want the subscriber to notified about.

Step 5 Click **Save**. At any point, click **Cancel** to creating the new email subscription for the tenant.

Edit Email Subscriptions

Before you begin

You must be an **Admin** to view the email subscription list, and a **SuperAdmin** to add, remove, or edit email subscriptions.

Procedure

Step 1 In the left pane, click **Administration** > **Notification Settings**.

Step 2 Locate the email addres you want to enable to edit for email subscriptions.

Step 3 Click the **Edit** icon.

Step 4 Edit the following attributes:

- Email address
- Send Alerts When.… Device Workflows
- Send Alerts When... Device Events
- Send Alerts When... Background Log Search

Step 5 Click **Ok**. At any point, click **Cancel** to negate any changes made to the email subscription.

Delete an Email Subscription

Use the following procedure to delete a mailer from the email subscription list.:

Before you begin

You must be an **Admin** to view the email subscription list, and a **SuperAdmin** to add, remove, or edit email subscriptions.

Procedure

Step 1 In the left pane, click **Administration** > **Notification Settings**.

Step 2 Locate the user you want to remove from email subscriptions for the tenant.

Step 3 Click the **Remove** icon for the user you want to remove.

Step 4 Confirm you want to remove the user from the subscription list. Note that this does not affect the user functionality in any way.

Enable Service Integrations for Security Cloud Control Notifications

Enable service integration to forward Security Cloud Control notifications through a specified messaging application or service. You need to generate a webhook URL from your messaging application and point Security Cloud Control to that webhook in Security Cloud Control's **Notification Settings** page to receive notifications.

Security Cloud Control natively supports Cisco Webex and Slack as service integrations. Messages sent to these services are specially formatted for channels and automated bots.

Note You must check the appropriate boxes for the notifications you want to receive per webhook.

Incoming Webhooks for Webex Teams

Before you begin

Security Cloud Control notifications appear in a designated workspace or as an automated bot in a private message. You must have the following before completing this procedure:

- A Webex account.
- A Security Cloud Control account and tenant.

Use the following procedure to allow incoming webhooks for Webex Teams:

Procedure

Step 1 Open the Webex apphub.

Step 2 Click **Connect** at the top of the page.

Step 3 Scroll to the bottom of the page and configure the following:

- **Webhook name** - Provide a name to identify the messages provided by this application.
- **Select a space** - Use the drop-down menu to choose a Webex **Space**. The Space must already exist in Webex team and you must have access to this space. If a space does not exist, you can create a new space in Webex Teams and refresh the application's configuration page to display the new space.

Note If a Webex incoming webhook has been configured in the past and you are re-enabling it, the previous webhooks are preserved at the bottom of this page. You can delete previous webhooks if they are no longer needed or if the Webex space no longer eists.

Step 4 Select **Add**. The Webex Space you chose will receive a notification that the application is added.

Step 5 Copy the Webhook URL.

Step 6 Log into Security Cloud Control.

Step 7 In the left pane, click **Administration** > **Notification Settings**.

Step 8 Examine and confirm the notifications that are checked are correct. If they are not, we strongly recommend modifiying the notification selection before you connect to a service integration.

Step 9 Scroll to **Service Integrations**.

Step 10 Click the blue plus button.

Step 11 Enter a **Name**. This name appears in Security Cloud Control as a configured service integration. It does not appear in any events forwarded to the configured service.

Step 12 Expand the drop-down menu and select **Webex** as the Service Type.

Step 13 Paste the webhook URL that you generated from the service.

Step 14 Click **OK**.

Incoming Webhooks for Slack

Security Cloud Control notifications appear in a designated channel or as an automated bot in a private message. For more information on how Slack handles incoming webhooks, see Slack Apps for more information.

Use the following procedure to allow incoming webhooks for Slack:

Procedure

Step 1 Log into your Slack account.

Step 2 In the panel to the left, scroll to the bottom and select **Add Apps**.

Step 3 Search application directory for **Incoming Webhooks** and locate the app. Select **Add**.

Step 4 If you are not the admin of your Slack workspace, you must send a request to the admin of your org and wait for the app to be added to your account. Select **Request Configuration**. Enter an optional message and select **Submit Request**.

Step 5 Once the Incoming Webhooks app is enabled for your workspace, refresh the Slack settings page and select **Add New Webhook to Workspace**.

Step 6 Use the drop-down menu to select the Slack channel you want the Security Cloud Control notifications to appear in. Select **Authorize**. If you navigate away from this page while waiting for the request to get enabled, simply log into Slack and select the workspace name in the upper left corner. From the drop-down menu, select **Customize Workspace** and select **Configure Apps**. Navigate to **Manage** > **Custom Integrations**. Select **Incoming Webhooks** to open app's landing page and then select **Configuration**from the tabs. This lists all the users within your workspace that has this app enabled. You can only see and edit your account's configuration. Select your workspace name to edit the configuration and move forward.

Step 7 The Slack settings page redirects you to the configuration page for the app. Locate and copy the webhook URL.

Step 8 Log into Security Cloud Control.

Step 9 In the left pane, click **Administration** > **Notification Settings**.

Step 10 Examine and confirm the notifications that are checked are correct. If they are not, we strongly recommend modifiying the notification selection before you connect to a service integration.

Step 11 Scroll to **Service Integrations**.

Step 12 Click the blue plus button.

Step 13 Enter a **Name**. This name appears in Security Cloud Control as a configured service integration. It does not appear in any events forwarded to the configured service.

Step 14 Expand the drop-down menu and select **Slack** as the Service Type.

Step 15 Paste the webhook URL that you generated from the service.

Step 16 Click OK.

Incoming Webhooks for a Custom Integration

Before you begin

Security Cloud Control does not format messages for custom integration. If you opt to integrate a custom service or application, Security Cloud Control sends a JSON message.

Refer to the service's documentation on how to enable incoming webhooks and generate a webhook URL. Once you have a webhook URL, use the procedure below to enable webhooks:

Procedure

Step 1 Generate and copy the webhook URL from the custom service or application of your choice.

Step 2 Log into Security Cloud Control.

Step 3 In the left pane, click **Administration** > **Notification Settings**.

Step 4 Examine and confirm the notifications that are checked are correct. If they are not, we strongly recommend modifiying the notification selection before you connect to a service integration.

Step 5 Scroll to **Service Integrations**.

Step 6 Click the blue plus button.

Step 7 Enter a **Name**. This name appears in Security Cloud Control as a configured service integration. It does not appear in any events forwarded to the configured service.

Step 8 Expand the drop-down menu and select **Custom** as the Service Type.

Step 9 Paste the webhook URL that you generated from the service.

Step 10 Click OK.

Logging Settings

View your monthly event logging limit and how many days are left until the limit resets. Note that stored logging represents the compressed event data that the Cisco cloud received.

Click **View Historical Usage** to see all of the logging your tenant has received over the past 12 months.

There are also links you can use to request additional storage.

Integrate Your SAML Single Sign-On with Security Cloud Control

Security Cloud Control uses Cisco Secure Sign-On as its SAML single sign-on identity provider (IdP) and Duo Security for multifactor authentication (MFA). This is Security Cloud Control's preferred authentication method.

If, however, customers want to integrate their own SAML single sign-on IdP solution with Security Cloud Control, they can as long as their IdP supports SAML 2.0 and identity provider-initiated workflow.

To integrate your own or third-party identity provider (IdP) with Cisco Security Cloud Sign On, see Cisco Security Cloud Sign On Identity Provider Integration Guide.

If you need more support to integrate your own SAML solution with Security Cloud Control, contact support and create a case.

Attention When you open a case, ensure that you choose **Manually Select A Technology** and select **SecureX - Sign-on and Administration** for your request to reach the right team.

Renew SSO Certificate

Your Identity Provider (IdP) is usually integrated with SecureX SSO. Open a Cisco TAC case and provide the metadata.xml file. For more information, see Cisco SecureX Sign-On Third-Party Identity Provider Integration Guide.

Attention When you open a case, ensure that you choose **Manually Select A Technology** and select **SecureX - Sign-on and Administration** for your request to reach the right team.

(legacy only) If your Identity Provider (IdP) integration is directly with Security Cloud Control, open a How Security Cloud Control Customers Open a Support Ticket with TAC and provide the metadata.xml file.

API Tokens

Developers use Security Cloud Control API tokens when making Security Cloud Control REST API calls. The API token must be inserted in the REST API authorization header for a call to succeed. API tokens are "long-lived" access tokens which do not expire; however, you can renew and revoke them.

You can generate API tokens from within Security Cloud Control. These tokens are only visible immediately after they're generated and for as long as the General Settings page is open. If you open a different page in Security Cloud Control and return to the **General Settings** page, the token is no longer visible, although it is clear that a token has been issued.

Individual users can create their own tokens for a particular tenant. One user cannot generate a token on behalf of another. Tokens are specific to an account-tenant pair and cannot be used for other user-tenant combinations.

API Token Format and Claims

The API token is a JSON Web Token (JWT). To learn more about the JWT token format, read the Introduction to JSON Web Tokens.

The Security Cloud Control API token provides the following set of claims:

- **id** - user/device uid
- **parentId** - tenant uid
- **ver** - the version of the public key (initial version is 0, for example, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - Security Services Exchange subscriptions (optional)
- **client_id** - "**api-client**"
- **jti** - token id

Token Management

Generate an API Token

Procedure

Step 1 From the drop-down list under your username, click **Preferences** > **General Preferences**.

Step 2 In My Tokens, click **Generate API Token**.

Step 3 Save the token in a secure location in accordance with your enterprise's best practices for maintaining sensitive data.

Renew an API Token

The API token does not expire. However, users may choose to renew their API token if the token is lost, compromised, or to conform to their enterprise's security guidelines.

Procedure

Step 1 From the drop-down list under your username, click **Preferences** > **General Preferences**.

Step 2 In My Tokens, click **Renew**. Security Cloud Control generates a *new* token.

Step 3 Save the new token in a secure location in accordance with your enterprise's best practices for maintaining sensitive data.

Revoke an API Token

Procedure

Step 1 From the drop-down list under your username, click **Preferences** > **General Preferences**.

Step 2 In My Tokens, click **Revoke**. Security Cloud Control revokes the token.

Relationship Between the Identity Provider Accounts and Security Cloud Control User Records

To log in to Security Cloud Control, a customer needs an account with a SAML 2.0-compliant identity provider (IdP), a multi-factor authentication provider, and a user record in Security Cloud Control. The IdP account contains the user's credentials and the IdP authenticates the user based on those credentials. Mutli-factor authentication provides an added layer of identity security. The Security Cloud Control user record primarily contains the username, the Security Cloud Control tenant with which they are associated, and the user's role. When a user logs in, Security Cloud Control tries to map the IdP's user ID to an existing user record on a tenant in Security Cloud Control. When Security Cloud Control finds a match, the user is logged in to that tenant.

Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Security Cloud Sign On. Cisco Security Cloud Sign On uses Duo for mutli-factor authentication. Customers can Integrate Your SAML Single Sign-On with Security Cloud Control if they choose.

Login Workflow

This is a simplified description of how the IdP account interacts with the Security Cloud Control user record to log in a Security Cloud Control user:

Procedure

Step 1 The user requests access to Security Cloud Control by logging in to a SAML 2.0-compliant identity provider (IdP) such as Cisco Security Cloud Sign On (https://sign-on.security.cisco.com) for authentication.

Step 2 The IdP issues a SAML assertion that the user is authentic, and a portal displays the applications the user can access. One of the tiles represents Security Cloud Control.

Step 3 Security Cloud Control validates the SAML assertion, extracts the username and attempts to find a user record among its tenants that corresponding to that username.

- If the user has a user record on a single tenant on Security Cloud Control, Security Cloud Control grants the user access to the tenant and the user's role determines the actions they can take.
- If the user has a user record on more than one tenant, Security Cloud Control presents the authenticated user with a list of tenants they can choose from. The user picks a tenant and is allowed to access the tenant. The user's role on that specific tenant determines the actions they can take.
- If Security Cloud Control does not have a mapping for the authenticated user to a user record on a tenant, Security Cloud Control displays a landing page giving users the opportunity to learn more about Security Cloud Control or request a free trial.

Creating a user record in Security Cloud Control does not create an account in the IdP and creating an account in the IdP does not create a user record in Security Cloud Control.

Similarly, deleting an account on the IdP does not mean you have deleted the user record from Security Cloud Control; although, without the IdP account, there is no way to authenticate a user to Security Cloud Control. Deleting the Security Cloud Control user record does not mean you have deleted the IdP account; although,

without the Security Cloud Control user record, there will be no way for an authenticated user to access a Security Cloud Control tenant.

Implications of this Architecture

Customers Who Use Cisco Security Cloud Sign On

For customers who use Security Cloud Control's Cisco Security Cloud Sign On identity provider, a Super Admin can create a user record in Security Cloud Control and a user can self-register themselves with Security Cloud Control. If the two usernames match, and the user is properly authenticated, the user can log in to Security Cloud Control.

Should the Super Admin ever need to prevent a user from accessing Security Cloud Control, they can simply delete the Security Cloud Control user's user record. The Cisco Security Cloud Sign On account will still exist and if the Super Admin ever wants to restore the user, they can by creating a new Security Cloud Control user record with the same username as the one used for Cisco Security Cloud Sign On.

Should a customer ever run into a problem with Security Cloud Control that requires a call to our Technical Assistance Center (TAC), the customer could create a user record for the TAC engineer so they could investigate the tenant and report back to the customer with information and suggestions.

Customers Who Have Their Own Identity Provider

For Integrate Your SAML Single Sign-On with Security Cloud Control, they control both the identity provider accounts and the Security Cloud Control tenants. These customers can create and manage identity provider accounts and user records in Security Cloud Control.

Should they ever need to prevent a user from accessing Security Cloud Control, they can delete the IdP account, the Security Cloud Control user record, or both.

If they ever need help from Cisco TAC, they can create both the identity provider account and a Security Cloud Control user record, with a read-only role, for their TAC engineer. The TAC engineer would then be able to access the customer's Security Cloud Control tenant, investigate, and report back the customer with information and suggestions.

Cisco Managed Service Providers

If Cisco Managed Service Providers (MSPs) use Security Cloud Control's Cisco Security Cloud Sign On IdP, they can self-register for Cisco Security Cloud Sign On and their customers can create a user record for them in Security Cloud Control so that the MSP can manage the customer's tenant. Of course, the customer has full control to delete the MSP's record when they choose to.

Related Topics

- General Settings
- Manage Users in Security Cloud Control
- User Roles in Security Cloud Control

Manage Multi-Tenant Portal

Security Cloud Control Multi-Tenant Portal view retrieves and displays information from all devices across multiple tenants. This multi-tenant portal shows the device status, software versions running on them, and many more.

Before you begin

- The multi-tenant portal is only available if the feature is enabled on your tenant. To enable multi-tenant portal for your tenant, open a support ticket with Cisco TAC.
- Once the support ticket is resolved and the portal is created, users with the **Super Admin** role on the portal have the ability to add tenants to it.
- We recommend you to clear cache and cookies from your web browser to avoid certain browser-related issues that may occur.

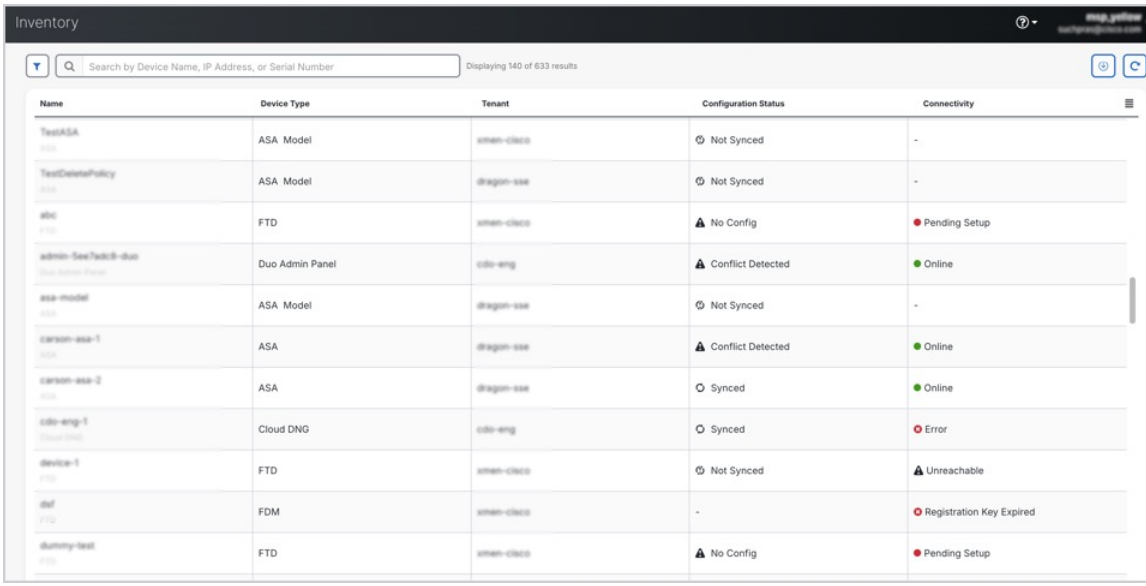
Multi-Tenant Portal

The portal provides the following menus:

- **Security Devices**
  - Displays all the devices onboarded to the tenants added to the portal. Use the **Search** and **Filter** options to search for devices.
  - You can click a device to view details such as **Model**, **Onboarding Method**, **Firewall Mode**, **Software Version**, and so on.
  - You can manage a device only from the Security Cloud Control tenant that manages it. The multi-tenant portal provides the **Manage devices** link that directs you to the Security Cloud Control tenant page.

    You can see this link if you have an account on that tenant, and the tenant is in the same region as the portal. If you don't have permission to access the tenant, you may not see the **Manage devices** link. Contact the Super Admin in your organization for permission.
  - You can export the details to a comma-separated value (.csv) file. This information helps you analyze the devices or send it to someone who doesn't have access. Every time you export the data, Security Cloud Control creates a new .csv file, where the file created has a date and time in its name.
  - The column picker allows you to select or clear the device properties to view in the table. If you customize the table, Security Cloud Control remembers your selection the next time you sign in.

Figure 3: Security Devices



Note If the tenant managing the device is in a different region, you see the link to sign in to Security Cloud Control in that region. If you don't have access to Security Cloud Control in that region or the tenant in that region, you will not be able to manage the device.

- **Tenants**
  - Displays all the tenants added to the portal.
  - Only users with **Super Admin** roles can add tenants to the portal.
  - You can search by tenant name and export the tenants' information to a comma-separated value (.csv) file.
- **Settings**
  - In **General Settings**, you can view the **Portal Settings** details.
  - In **User Management**, you can view a list of all **Users**, **Active Directory Groups**, and **Audit Logs**. For more information, see User Management.

Note If you are a multitenant portal Super Admin, you can use API endpoints to:

- Create a Security Cloud Control tenant
- Add an existing Security Cloud Control tenant to the multitenant portal

Add a Tenant to a Multi-Tenant Portal

A user with the **Super Admin** role can add tenants to the portal. You can add tenants across multiple regions. For example, you can add a tenant from the Europe region into the US region and conversely.

Important We recommend that you Create API Only Users for your tenant and generate an API token for authenticating to Security Cloud Control.

Note If you want to add multiple tenants to the portal, generate API tokens from each tenant and paste them into a text file. You can then easily add the tenants one after another to the portal without switching to the tenant every time to generate a token.

Procedure

Step 1 In the left pane, click **Tenants**.

Step 2 Click **Add Tenant**.

Step 3 To add a new tenant, click **Next**.

Note

a. To import existing tenants, check the **Would you like to import existing tenant?** checkbox.

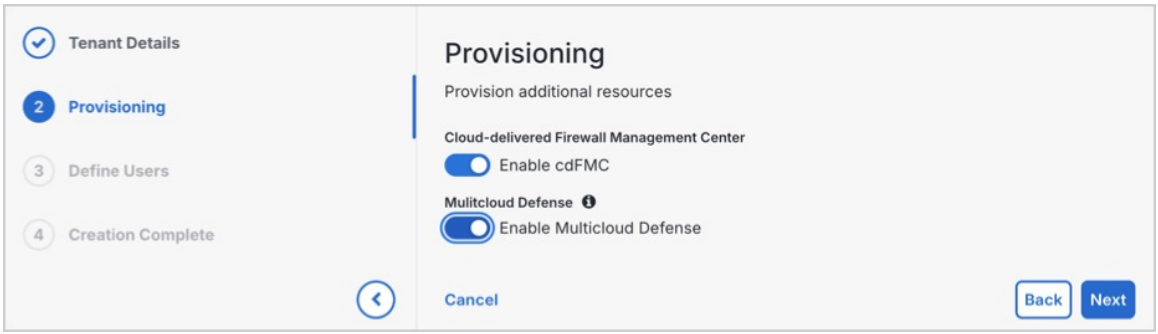
b. Add existing tenants from Security Cloud Control by pasting multiple API tokens separated by commas.

c. Click **Import**.

Step 4 Under **Tenant Details**, enter the **Display Name** and **Tenant Name**. Click **Next.**

Step 5 Under **Provisioning**,

- Enable the **Enable Multicloud Defense** toggle to provision multicloud defense for your tenant.
- Enable the **Enable Cloud-delivered Firewall Management Center** toggle to provision cloud-delivered Firewall Management Center for your tenant.
- Click **Next**.



Step 6 Under **Define Users**, either add users manually one by one, or download the CSV template, fill in the necessary details, and upload the file. Added users are displayed in the **User list** section.

Step 7 Click **Create Tenant**.

Tenant creation is complete, and provisioning may take a few minutes.

Delete a Tenant from a Multi-Tenant Portal

Procedure

Step 1 In the left pane, click **Tenants**.

Step 2 Click the corresponding delete icon appearing on the right to remove the tenant that you want.

Step 3 Click **Remove**. Note that the associated devices are also removed from the portal.

Manage-Tenant Portal Settings

Security Cloud Control enables to customize certain aspects of your Multi-Tenant Portal and individual user accounts on the Settings page. Access the settings page by clicking **Settings** in the left pane.

Settings

General Settings

Web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous, and no sensitive data is transmitted.

Web analytics is enabled by default. To disable web analytics or to enable in the future, follow this procedure:

1. In the left pane, click **Administration** > **General Settings**.
2. Click the slider under **Web Analytics**.

User Management

You can see all the user records associated with the Mult-Tenant Portal on the **User Management** screen. You can add, edit, or delete a user account. For more information, see Manage Users in Security Cloud Control.

Switch Tenant

If you have more than one portal tenants, you can switch between different portal or tenants without signing out from Security Cloud Control.

Procedure

Step 1 On the multi-tenant portal, click your tenant menu appearing on the top right corner.

Step 2 Click **Switch tenant**.

Step 3 Choose the portal or tenant that you want to view.

The Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the device and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the device and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that might be available for your product.
- To help Cisco improve our products.

The device establishes and maintains the secure connection at all times, and allows you to enroll in the Cisco Success Network. After you have registered the device, you can change the Cisco Success Network setting.

Note

- For threat defense high availability pairs, the selection of the active device overrides the Cisco Success Network setting on the standby device.
- Security Cloud Control does not manage the Cisco Success Network settings. The settings managed through, and telemetry information is provided by, the Firewall Device Manager user interface.

Enable or Disable the Cisco Success Network

During initial system setup, you are prompted to register the device with Cisco Smart Software Manager. If you instead elected to use the 90-day evaluation license, you must register the device before the end of the evaluation period. To enroll the device, either register the device with Cisco Smart Software Manager (on the Smart Licensing page) or enroll with Security Cloud Control by entering a registration key.

When you register the device, your virtual account allocates the license to the device. Registering the device also registers any optional licenses that you have enabled.

You can turn off this connection at any time by disabling Cisco Success Network, although you can only disable this option through the Firewall Device Manager UI. Disabling will disconnect the device from the cloud. Disconnection does not impact the receipt of updates or the operation of the Smart Licensing capabilities, which continue to operate normally. See the **Connecting to the Cisco Success Network** section of the System Administration chapter of the Firepower Device Manager configuration Guide, Version 6.4.0 or later for more information.

Manage Users in Security Cloud Control

Before you create or edit a user record in Security Cloud Control, read Relationship Between the Identity Provider Accounts and Security Cloud Control User Records to learn how the identity provider (IdP) account and the user record interact. Security Cloud Control users need a record and a corresponding IdP account so they can be authenticated and access the Security Cloud Control tenant.

Unless your enterprise has its own IdP, Cisco Secure Sign-On is the identity provider for all Security Cloud Control tenants. The rest of this article assumes you are using Cisco Secure Sign-On as your identity provider.

You can see all the user records associated with your tenant on the **User Management** screen. This includes any Cisco support engineer who is temporarily associated with your account to resolve a support ticket.

View the User Records Associated with your Tenant

Procedure

In the left pane, **Administration** > **User Management**.

Note To prevent Cisco support from accessing your tenant, enable the **Prevent Cisco support from viewing this tenant** toggle in the General Settings page.

Active Directory Groups in User Management

For tenants that have a high turnover for large quantities of users, you can map Security Cloud Control to your Active Directory (AD) groups instead of adding individual users to Security Cloud Control for an easier way to manage your user lists and user roles. Any user changes, such as a new user addition or removing existing users, can now be done in Active Directory and no longer need to be done in Security Cloud Control.

You must have a **SuperAdmin** user role to add, edit, or delete an Active Directory group from the **User Management** page. See User Roles in Security Cloud Control for more information.

In the left pane, choose **Settings** > **User Management**

Active Directory Groups

- In the left pane, click **Administration** > **User Management > Active Directory Groups**.
- This page displays the role of the Active Directory group as assigned in your Active Directory manager.
- Users within an Active Directory group are not listed individually in either the **Active Directory Groups** tab or the **Users** tab.

Audit Logs

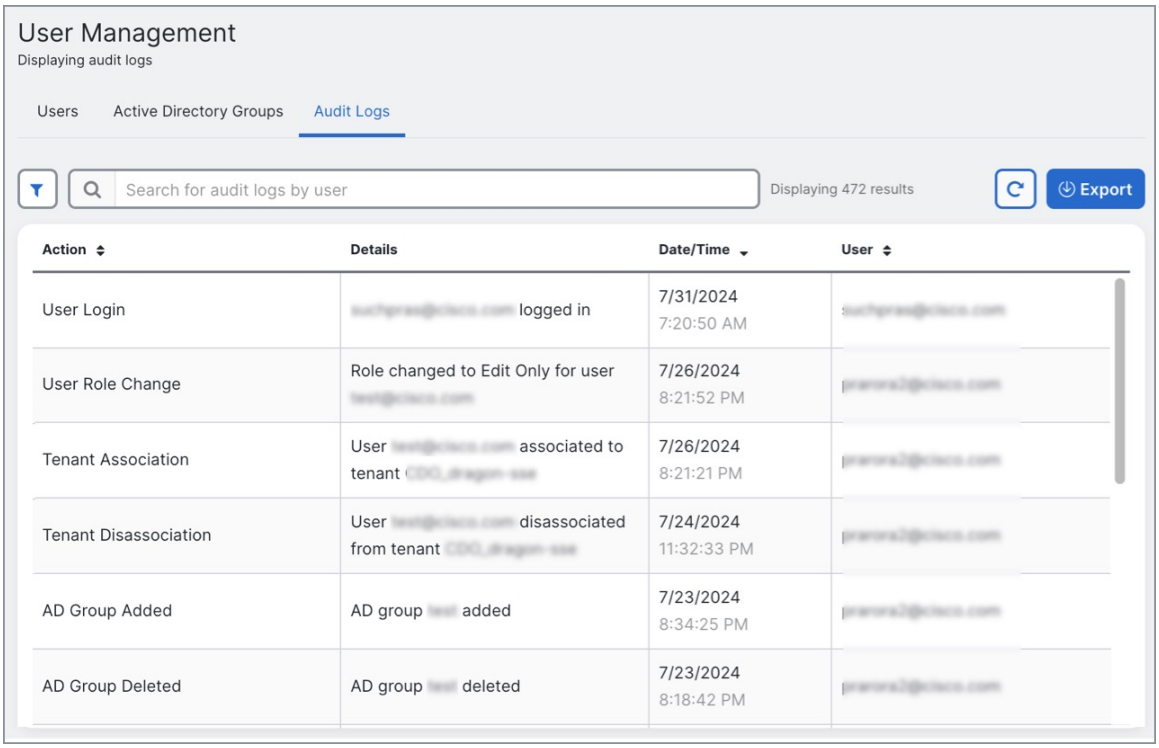
Audit Logs in Security Cloud Control record user-related and system-level actions. Key events that are captured by the **Audit Logs** include:

- **User Login:** Records every instance of user authentication.
- **Tenant Association and Disassociation:** Tracks user associations with, or disassociations from, tenants.
- **User Role Change:** Records any modifications to user roles.
- **Active Directory Groups:** Records any addition, deletion, and role changes within AD groups.

Procedure:

1. In the left pane, click **Administration** > **User Management**.
2. Click the **Audit Logs** tab. A list of events and activities in the current tenant you are logged into is displayed.
3. Use the **Search** text box to find logs for a specific user.
4. Click the filter icon to refine your search results and view specific events. You can filter the logs based on the **Time Range** and **Event Action**.
5. Click **Export** to download the details in CSV format.

Figure 4: Audit Logs



Multi-role Users

As an extension along the IAM capabilities in Security Cloud Control, it is now possible for a user to have multiple roles.

A user can be part of multiple groups in Active Directory, and those groups can be defined in Security Cloud Control with different Security Cloud Control roles. The final permissions that a user gets on login are a combination of the roles of all the Active Directory groups that are defined in Security Cloud Control that the user is part of. For instance, if a user is part of two Active Directory groups and both the groups are added in Security Cloud Control with two different roles such as edit-only and deploy-only, the user would have both edit-only and deploy-only permissions. This applies to any number of groups and roles.

Active Directory group mappings must only be defined one time in Security Cloud Control, and managing access and permissions for users can after be achieved exclusively in Active Directory by adding, removing, or moving users between different groups.

Note If a user is both an individual user and part of an Active Directory group on the same tenant, the user role of the individual user overrides the user role of the Active Directory group.

API Endpoints for Active Directory Groups

If you are a super admin, you can use API endpoints to do the following:

- Create an Active Directory group
- Remove an Active Directory group
- Modify an Active Directory group
- Get Active Directory groups
- Get an Active Directory group

The aforementioned links point to the corresponding sections of the Cisco DevNet website.

Prerequisites for Adding an Active Directory Group to Security Cloud Control

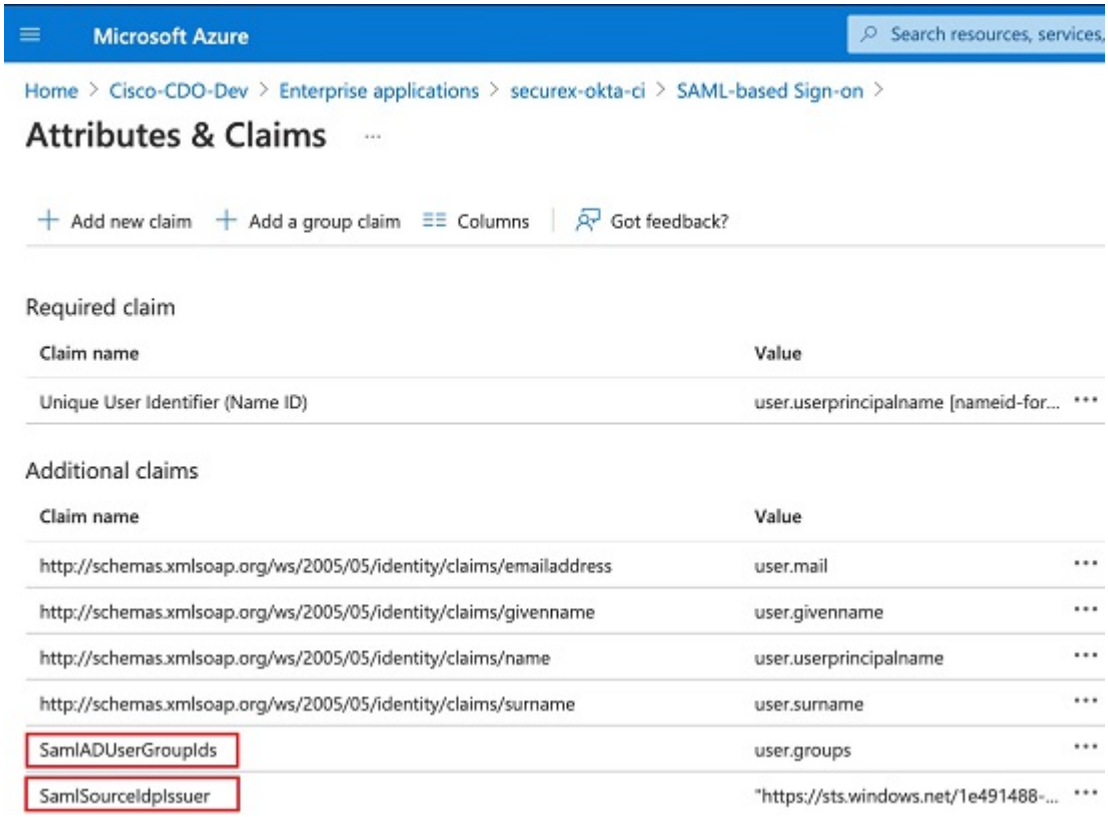
Before adding an Active Directory group mapping to Security Cloud Control as a form of user management, you must have your Active Directory that is integrated with Security Cloud Sign On. If your Active Directory Identity Provider (IdP) is not already integrated, see identity provider integration guide to integrate a custom Active Directory IdP integration with the following information:

- Your Security Cloud Control tenant name and region
- Domain to define custom routing for (for example: @cisco.com, @myenterprise.com)
- Certificate and federation metadata in the XML format

After your Active Directory integration is complete, add the following custom SAML claims in your Active Directory. The SAML claims and attributes are required, for you to be able to successfully sign-in to your Security Cloud Control tenant after your Active Directory integration is done. These values are case sensitive:

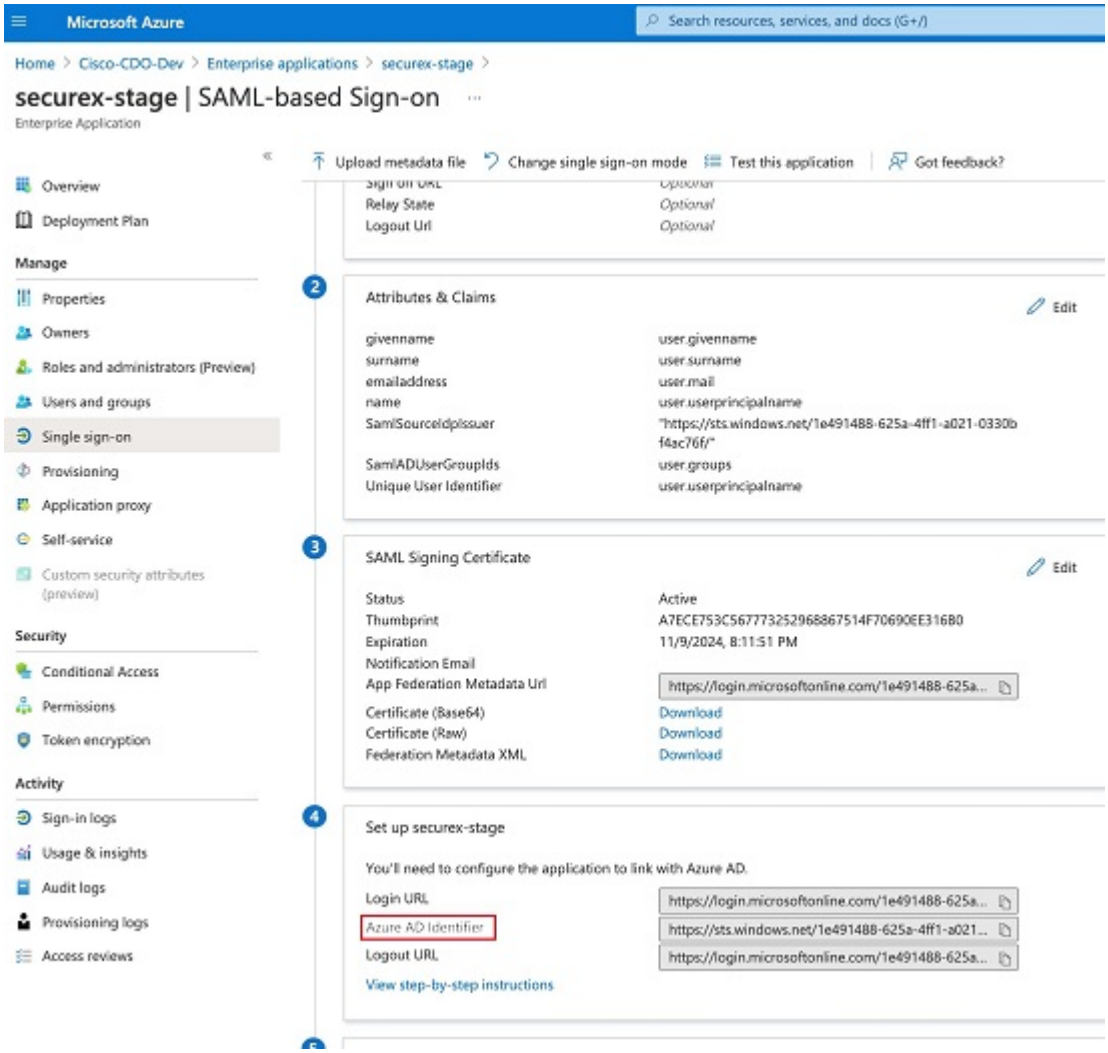
- **SamlADUserGroupIds** - This attribute describes all group associations that a user has on Active Directory. For example, in Azure select **+ Add a group claim** as seen in the screenshot below:

Figure 5: Custom Claims Defined in Active Directory



- **SamlSourceIdpIssuer** - This attribute uniquely identifies an Active Directory instance. For example, in Azure select **+ Add a group claim** and scroll to locate the Azure Active Directory Identifier as seen in the screenshot below:

Figure 6: Locate the Azure Active Directory Identifier



Add an Active Directory Group for User Management

You must have a **SuperAdmin** user role to add, edit, or delete an Active Directory group.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **User Management**.

Step 3 Click the **Active Directory Groups** tab.

Step 4 Click the add Active Directory group (+) button.

Step 5 Provide the following information:

- **Group Name**: Enter a unique name. This name does not have to match the group name in your Active Directory. Security Cloud Control does not support special characters for this field.
- **Group Identifier**: Manually enter the Group Identifier from your Active Directory. The value of the group identifier should be the same as the group identifier in the custom claim definition. It could be any value that corresponds to the unique identity of the group, for example, my-favourite-group, 12345, and so forth.
- **AD Issuer**: Manually enter the Active Directory Issuer value from your Active Directory.
- **Role**: Select a user role. This determines the role for all the users included in this Active Directory group. See User Roles in Security Cloud Control for more information.
- (Optional) **Notes**: Add any notes that are applicable to this Active Directory group.

Step 6 Select **OK**.

Edit an Active Directory Group for User Management

Before you begin

Note that editing an Active Directory Group's user management in Security Cloud Control only allows you to modify how Security Cloud Control limits the Active Directory group. You cannot edit the Active Directory group itself in Security Cloud Control. You must use Active Directory to edit the list of users within an Active Directory group.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **User Management**.

Step 3 Click the **Active Directory Groups** tab.

Step 4 Identify the Active Directory Group you want to edit and click the edit icon.

Step 5 Modify the following values:

- **Group Name**: Enter a unique name. Security Cloud Control does not support special characters for this field.
- **Group Identifier**: Manually enter the Group Identifier from your Active Directory. The value of the group identifier should be the same as the group identifier in the custom claim definition. It could be any value that corresponds to the unique identity of the group, for example, my-favourite-group, 12345 and so forth.
- **AD Issuer**: Manually enter the Active Directory Issuer value from your Active Directory.
- **Role**: This determines the role for all the users included in this Active Directory group. See User Roles for more information.
- **Notes**: Add any notes that are applicable to this Active Directory group.

Step 6 Click **OK**.

Delete an Active Directory Group for User Management

Procedure

Step 1 Log in to Security Cloud Control.
Step 2 In the left pane, click **Administration** > **User Management**.
Step 3 Click the **Active Directory Groups** tab.
Step 4 Identify the Active Directory Group you want to delete.
Step 5 Click the delete icon.
Step 6 Click **OK** to confirm you want to delete the Active Directory group.

Create a New Security Cloud Control User

These two tasks are necessary for creating a new Security Cloud Control user. They do not have to be done in sequence:

- Create a Cisco Security Cloud Sign On Account for the New User
- Create a User Record with Your Security Cloud Control Username

After these tasks are done, then the user can The New User Opens Security Cloud Control from the Cisco Secure Sign-On Dashboard.

Create a Cisco Security Cloud Sign On Account for the New User

Creating a Cisco Security Cloud Sign On account can be done by the new user at any time, without needing to know the name of the assigned tenant.

About Logging in to Security Cloud Control

Security Cloud Control uses Cisco Secure Sign-On as its identity provider and Duo for multi-factor authentication (MFA). **To log into Security Cloud Control, you must first create your account in Cisco Security Cloud Sign On and configure MFA using Duo**.

Security Cloud Control requires MFA which provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into Security Cloud Control. The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand.

Important **If your Security Cloud Control tenant existed before October 14, 2019**, use Migrate to Cisco Security Cloud Sign On Identity Provider, on page 9 for log in instructions instead of this article.

Before You Log In

Install DUO Security

We recommend installing the Duo Security app in a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.

Time Synchronization

You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock set automatically or manually set it to the correct time.

Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication

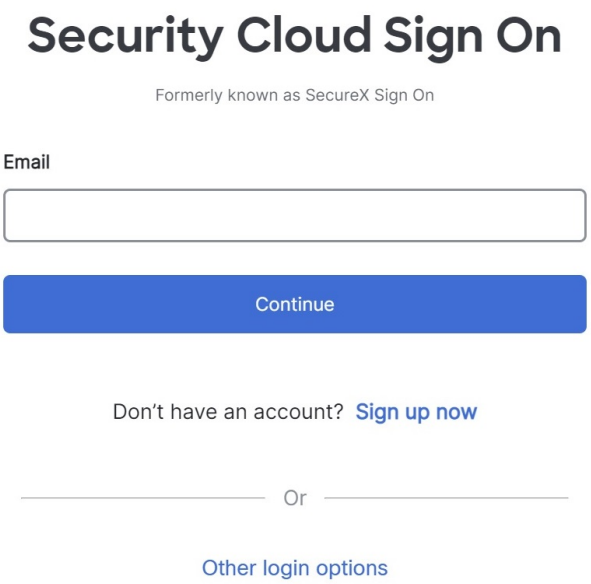
The initial sign-on workflow is a four-step process. You need to complete all four steps.

Procedure

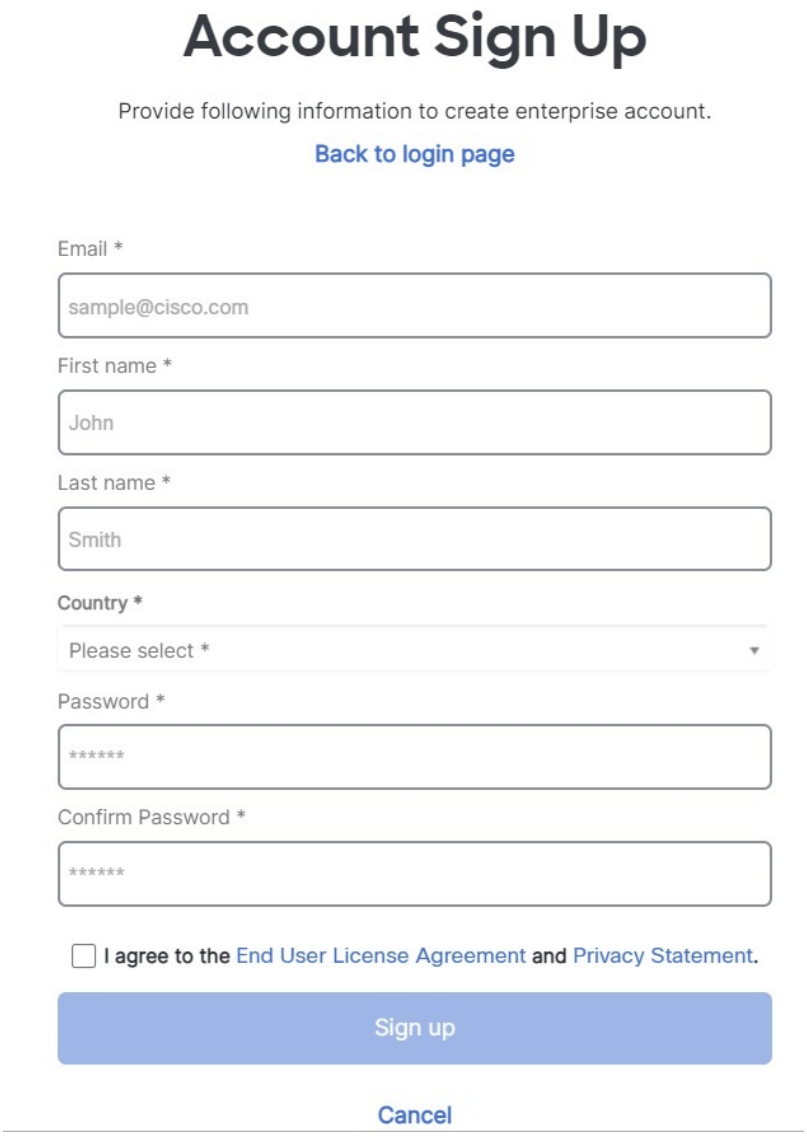
Step 1 **Sign Up for a New Cisco Security Cloud Sign On Account**.

a. Open https://sign-on.security.cisco.com.

b. At the bottom of the sign in screen, click **Sign up now**.



c. Provide the following information to create enterprise account.



Here are some tips:

- **Email**: Enter the email address that you will eventually use to log in to Security Cloud Control.
- **Password**: Enter a strong password.

d. Click **Sign up**.

Cisco sends you a verification email to the address you registered with. Open the email and click **Activate account**.

Step 2 **Set up Multi-factor Authentication Using Duo**

We recommend using a mobile device when setting up multi-factor authentication.

a. In the **Set up multi-factor authentication** screen, click **Configure factor**.

b. Click **Start setup** and follow the prompts to choose a mobile device and verify the pairing of that mobile device with your account.

For more information, see Duo Guide to Two Factor Authentication: Enrollment Guide. If you already have the Duo app on your device, you'll receive an activation code for this account. Duo supports multiple accounts on one device.

c. At the end of the wizard click **Continue to Login**.

d. Log in to Cisco Security Cloud Sign On with the two-factor authentication.

Step 3 **(Optional) Setup Google Authenticator as an additional authenticator**

a. Choose the mobile device you are pairing with Google Authenticator and click **Next**.

b. Follow the prompts in the setup wizard to setup Google Authenticator.

Step 4 **Configure Account Recovery Options for your Cisco Security Cloud Sign On**

a. Choose a recovery phone number for resetting your account using SMS.

b. Choose a security image.

c. Click **Create My Account**.

Create a User Record with Your Security Cloud Control Username

Only a Security Cloud Control user with **Super Admin** privileges can create the Security Cloud Control user record. The **Super Admin** must create the user record with the same email address that was specified in the **Create Your Security Cloud Control Username** task above.

Use the following procedure to create a user record with an appropriate user role:

Procedure

Step 1 Login to Security Cloud Control.

Step 2 In the left pane, choose **Settings** > **User Management**.

Step 3 Click  to add a new user to your tenant.

Step 4 Provide the email address of the user.

Note The user's email address must correspond to the email address of the Cisco Secure Log-On account.

Step 5 From the **Role** drop-down list, select the user's User Roles in Security Cloud Control.

Step 6 Click **OK**.

The New User Opens Security Cloud Control from the Cisco Secure Sign-On Dashboard

Procedure

Step 1 Click the appropriate **Security Cloud Control** tile on the Cisco Secure Sign-on dashboard for your tenant's region.

Step 2 Click the authenticator logo to choose Duo Security or Google Authenticator if you have set up both authenticators.

- If you already have a user record on an existing tenant, you are logged into that tenant.
- If you already have a user record on several portals, you will be able to choose which portal to connect to.
- If you already have a user record on several tenants, you will be able to choose which Security Cloud Control tenant to connect to.
- If you do not already have a user record on an existing tenant, you will be able to learn more about Security Cloud Control or request a trial tenant.

The **Portals** view retrieves and displays consolidated information from multiple tenants. See Manage Multi-Tenant Portal for more information.

The **Tenant** view shows several tenants on which you have a user record.

User Roles in Security Cloud Control

There are a variety of user roles in Security Cloud Control: Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a Security Cloud Control user has access to more than one tenant, they may have the same user ID but different roles on different tenants. A user may have a read-only role on one tenant and a Super Admin role on another. When the interface or the documentation refers to a Read-only user, an Admin user, or a Super Admin user we are describing that user's permission level on a particular tenant.

Read-only Role

A user assigned the Read-Only role sees this blue banner on every page:

Users with the Read-Only role can do the following:

- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a read-only user revokes their own token, they cannot recreate it.
- Contact support through our interface and can export a change log.

Read-Only users **cannot** do the following:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Edit-Only Role

Users with the Edit-Only role can do the following:

- Edit and save device configurations, including but not limited to objects, policies, rulesets, interfaces, VPN, etc.
- Allow configuration changes that are made through the **Read Configuration** action.
- Utilize the Change Request Management action.

Edit-Only users **cannot** do the following:

- Deploy changes to a device or to multiple devices.
- Discard staged changes or changes that are detected through OOB.
- Upload AnyConnect Packages, or configure these settings.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create Security Cloud Control user records.
- Change user role.

Deploy-Only Role

Users with the Deploy-Only role can do the following:

- Deploy staged changes to a device, or to multiple devices.
- Revert or restore configuration changes for ASA devices.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Utilize the Change Request Management action.

Deploy-Only users **cannot** do the following:

- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create, update, configure, or delete anything on any page.

- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

VPN Sessions Manager Role

The VPN Sessions Manager role is designed for administrators monitoring remote access VPN connections, not site to site VPN connections.

Users with the VPN Sessions Manager role can do the following:

- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see RA VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a VPN Sessions Manager user revokes their own token, they cannot recreate it.
- Contact support through our interface and export a change log.
- Terminate existing RA VPN sessions.

VPN Sessions Manager users **cannot** do the following:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Admin Role

Admin users have complete access to most aspects of Security Cloud Control. Admin users can do the following:

- Create, read, update, and delete any object or policy in Security Cloud Control and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.

- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can contact support through our interface and can export a change log.

Admin users **cannot** do the following:

- Create Security Cloud Control user records.
- Change user role.

Super Admin Role

Super Admin users have complete access to all aspects of Security Cloud Control. Super Admins can do the following:

- Change a user role.
- Create user records.

Note Though Super Admins can create a Security Cloud Control user record, that user record is not all that is needed for a user to log in to your tenant. The user also needs an account with the identity provider used by your tenant. Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Security Cloud Sign On. Users can self-register for their Cisco Security Cloud Sign On account; see Initial Login to Your New Security Cloud Control Tenant, on page 8 for more information.

- Create, read, update, and delete any object or policy in Security Cloud Control and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can
- Contact support through our interface and can export a change log.

Change The Record of the User Role

The user record is the currently recorded role of a user. By looking at the users associated with your tenant, you can determine what role each use has by their record. By changing a user role, you change the user record. User's roles are identified by their role in the User Management table. See Manage Users in Security Cloud Control for more information.

You must be a Super Admin to change the user record. If your tenant has no Super Admins, contact How Security Cloud Control Customers Open a Support Ticket with TAC.

Add a User Account to Security Cloud Control

Security Cloud Control users need a Security Cloud Control record and a corresponding IdP account so they can be authenticated and access your Security Cloud Control tenant. This procedure creates the user's Security Cloud Control user record, not the user's account in Cisco Security Cloud Sign On. If the user does not have an account in Cisco Security Cloud Sign On, they can self-enroll by navigating to https://sign-on.security.cisco.com and clicking **Sign up** at the bottom of the Sign in screen.

Note You will need to have the role of Super Admin Role on Security Cloud Control to perform this task.

Create a User Record

Use the following procedure to create a user record with an appropriate user role:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **User Management**.

Step 3 Click the blue plus button () to add a new user to your tenant.

Step 4 Provide the email address of the user.

Note The user's email address must correspond to the email address of the Cisco Secure Log-On account.

Step 5 Select the user's User Roles in Security Cloud Control from the drop-down menu.

Step 6 Click **v**.

Note Though Super Admins can create a Security Cloud Control user record, that user record is not all that is needed for a user to log in to your tenant. The user also needs an account with the identity provider used by your tenant. Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Secure Sign-on. Users can self-register for their Cisco Secure Sign-On account; see Initial Login to Your New Security Cloud Control Tenant, on page 8 for more information.

Create API Only Users

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **User Management**.

Step 3 Click the blue plus button ( ) to add a new user to your tenant.

Step 4 Select the **API Only User** checkbox.

Step 5 In the **Username** field, enter a name for the user and click **OK**.

Important the user name can't be an email address or contain the '@' character as the '@yourtenant' suffix will be automatically appended to the user name.

Step 6 Select the user's User Roles in Security Cloud Control from the drop-down menu.

Step 7 Click **OK**.

Step 8 Click the **User Management** tab.

Step 9 In the **Token** column for the new API Only user, click **Generate API Token** to obtain an API token.

Edit a User Record for a User Role

You will need to have the role of Super Admin to perform this task. If the Super Admin changes the role of a Security Cloud Control user that is logged in, once their role has been changed, the user is automatically logged out of their session. Once the user logs back in, they assume their new role.

Note You will need to have the role of Super Admin Role on Security Cloud Control to perform this task.

Caution Changing the role of a user record will delete an API Tokens associated with the user record if there is one. The user must generate a new API token once the user role changes.

Edit a User Role

Note If a Security Cloud Control user is logged in, and a Super Admin changes their role, the user must log out and log back in again for the change to take affect.

To edit the role defined in the user record, follow this procedure:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **User Management**.

Step 3 Click the edit icon in the user's row.

Step 4 Select the user's new User Roles in Security Cloud Control from the Role drop-down menu.

Step 5 If the user record shows that there is an API token associated with the user, you will need to confirm that you want to change the user's role and delete the API token as a result.

Step 6 Click **v**.

Step 7 If Security Cloud Control deleted the API token, contact the user so that they may create a new API Token.

Delete a User Record for a User Role

Deleting a user record in Security Cloud Control prevents the associated user from logging in to Security Cloud Control by breaking the mapping of the user record with the Cisco Security Cloud Sign On account. When you delete a user record, you are also deleting the API token associated with that user record should there be one. Deleting a user record in Security Cloud Control does not delete the user's IdP account in Cisco Security Cloud Sign On.

Note You will need to have the role of Super Admin Role on Security Cloud Control to perform this task.

Delete a User Record

To delete the role defined in the user record, see the following procedure:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **User Management**.

Step 3 Click the trash can icon in the row of the user you want to delete.

Step 4 Click **OK**.

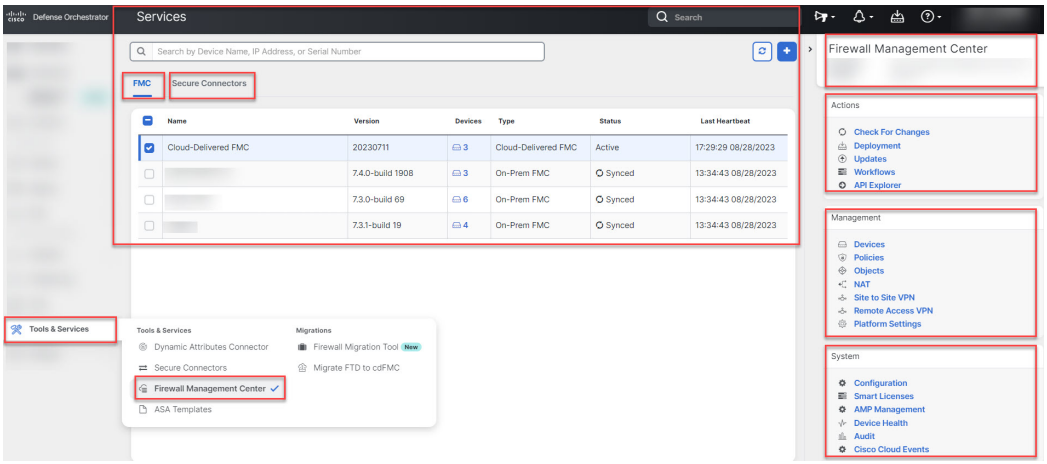
Step 5 Confirm that you want to remove the account from the tenant by clicking OK.

Security Cloud Control Services Page

The **Services** page displays a list of services that Security Cloud Control provides. Selecting the **FMC** tab lists the cloud-delivered Firewall Management Center that is linked to the Security Cloud Control account and all the on-premises management centers onboarded to Security Cloud Control. The devices that are managed by these on-prem management centers are listed in the **Inventory** page. The **Services** page also lists the secure connectors under the **Secure Connectors** tab.

You can click the **FMC** tab and onboard an on-premises management center by clicking the blue plus icon (), and perform device actions using the options in the right pane. You can also see device information such as version, number of devices being managed by the management center, device type, and the synchronization status of the device. Clicking on the managed devices icon takes you to the **Inventory** page, where devices managed by the selected on-premises management center are filtered automatically and displayed. The **Services** page also allows you to select more than one on-premises management center at a time for you to perform actions on a group of management centers all at once. You cannot select any on-premises management center while the cloud-delivered Firewall Management Center is selected. To add a new secure connector or perform actions on existing secure connectors, choose the **Secure Connectors** tab and click  .

Navigate **Administration** > **Integrations & Migration** > **Cloud Services**.



For your cloud-delivered Firewall Management Center, the Services page displays the following information:

- If you do not have a cloud-delivered Firewall Management Center deployed on your tenant, click **Enable Cloud-Delivered FMC**. See Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant for more information.
- The number of Secure Firewall Threat Defense devices deployed on the cloud-delivered Firewall Management Center.
- Status of the connection between Security Cloud Control and the cloud-delivered Firewall Management Center page.
- The last heartbeat of the cloud-delivered Firewall Management Center. This represents the last time the status of the cloud-delivered Firewall Management Center itself and the number of devices that it manages were synchronized with the table on this page.

- The hostname of the selected cloud-delivered Firewall Management Center.

Choose **Cloud-Delivered FMC** and using the links in the **Actions**, **Management**, or **Settings** pane, you open the cloud-delivered Firewall Management Center user interface to perform the configuration tasks that are associated with the link you clicked.

Actions:

- **Check For Changes**: The Device Count and Status information in the table will be updated with the information available the last time this page and the cloud-delivered Firewall Management Center were synchronized. Synchronization happens every 10 minutes.
- **Deployment**: Takes you to the device configuration deployment page on cloud-delivered Firewall Management Center. See Deploy Configuration Changes.
- **Workflows**: Takes you to the **Workflows** page to monitor every process that Security Cloud Control runs when communicating with devices. See Workflows page.
- **API Explorer**: Takes you to the page that lists the cloud-delivered Firewall Management Center REST APIs. See Secure Firewall Management Center REST API Guide.

Management:

- **Devices**: Takes you to the threat defense device listing page on the cloud-delivered Firewall Management Center portal. See Configure Devices.
- **Policies**: Takes you to the policies page on the cloud-delivered Firewall Management Center portal to edit system-provided access control policies and create custom access control policies. See Manage Access Control Policies.
- **Objects**: Takes you to the policies page on the cloud-delivered Firewall Management Center portal to manage reusable objects. See Object Management.
- **NAT**: Takes you to the policies page on the cloud-delivered Firewall Management Center portal to configure Network Address Translation policies on the threat defense devices. See Manage NAT policies.
- **Site to Site VPN**: Takes you to the site-to-site VPN dashboard page on the cloud-delivered Firewall Management Center portal to configure site-to-site VPN policy between two sites. See Site-to-Site VPNs.
- **Remote Access VPN**: Takes you to the remote access VPN dashboard page on the cloud-delivered Firewall Management Center portal to configure a remote access VPN configuration. See Remote Access VPN.
- **Platform Settings**: Takes you to the platform settings page on the cloud-delivered Firewall Management Center portal configure a range of unrelated features whose values you might want to share among several devices. See Platform Settings.

System:

- **Configuration**: Takes you to the system configuration settings page on the cloud-delivered Firewall Management Center portal to configure system configuration settings. See System Configuration.
- **Smart Licenses**: Takes you to the smart licenses page on the cloud-delivered Firewall Management Center portal to assign licenses to devices. See Assign Licenses to Devices.

- **AMP Management**: Takes you to the AMP management page on the cloud-delivered Firewall Management Center portal that provides intelligence that the system uses to detect and block malware on your network. See Cloud Connections for Malware Protection.
- **Device Health**: Takes you to the health monitoring page on the cloud-delivered Firewall Management Center portal that tracks various health indicators to ensure that the hardware and software in the system are working correctly. See About Health Monitoring.
- **Audit**: Takes you to the audit log page on the cloud-delivered Firewall Management Center portal to show the generated audit record for each user interaction with the web interface.
- **Cisco Cloud Events**: Takes you to the configure Cisco Cloud events page on the Security Cloud Control portal to configure cloud-delivered Firewall Management Center to send events directly to SAL (SaaS). See Send Events to SAL (SaaS).

After opening the cloud-delivered Firewall Management Center page, click the blue question mark button and select **Page-level Help** to learn more about the page you are on and what further action you can take.

Support to Open Security Cloud Control and Cloud-delivered Firewall Management Center Applications on Different Tabs

As you configure threat defense devices or objects in the cloud-delivered Firewall Management Center, you can open the appropriate configuration pages in additional browser tabs to work simultaneously in the Security Cloud Control and the cloud-delivered Firewall Management Center portals without logging off. For example, you can create an object on the cloud-delivered Firewall Management Center and simultaneously monitor event logs on Security Cloud Control that are generated from the security policies.

This feature is available for all Security Cloud Control links that navigate to the cloud-delivered Firewall Management Center portal. To open the cloud-delivered Firewall Management Center portal in a new tab:

On the Security Cloud Control portal, press and hold the **Ctrl** (Windows) or **Command** (Mac) button, then click the corresponding link.

Note A single click opens the cloud-delivered Firewall Management Center page in the same tab.

Here are some examples of opening the cloud-delivered Firewall Management Center portal page in a new tab:

- Choose **Tools & Services** > **Firewall Management Center** and select **Cloud-Delivered FMC**.

  In the right pane, press and hold the **Ctrl** (Windows) or **Command** (Mac) button, and then click the page that you want to access.

- Choose **Objects** > **Other FTD Objects**.
- Click the search icon in the top-right corner of the Security Cloud Control page and enter the search strings in the search field that appears.

  From the search result, press and hold the **Ctrl** (Windows) or **Command** (Mac) button, and then click the arrow icon.

- Choose **Dashboard** > **Quick Actions**.

  Press and hold the **Ctrl** (Windows) or **Command** (Mac) button, and then click **Manage FTD Policies** or **Manage FTD Objects**.

Note When you switch to a new Security Cloud Control tenant, the corresponding cloud-delivered Firewall Management Center portal already opened in a new tab logs out.

Related Topics

- Managing On-Prem Firewall Management Center with Cisco Security Cloud Control
- Onboard an On-Prem Firewall Management Center
- Request a cloud-delivered Firewall Management Center for your Security Cloud Control tenant
- Secure Device Connector
- Secure Event Connectors

Security Cloud Control Device and Service Management

Security Cloud Control provides the ability to view, manage, filter, and evaluate your onboarded devices on the **Inventory** page. From the **Inventory** page you can:

- Onboard devices and services for Security Cloud Control management.
- View the configuration state and connectivity state of managed devices and services.
- View onboarded devices and templates categorized in separate tabs. See Security Cloud Control Inventory Information, on page 101.
- Evaluate and take action on individual devices and services.
- View device and service specific information and resolve issues.
- View device health status for threat defense devices managed by:
  - cloud-delivered Firewall Management Center
  - on-premises management center

  For threat defense devices managed by the cloud-delivered Firewall Management Center, you can also see the node status for devices in a cluster.
- Search for a device or template by name, type, IP address, model name, serial number, or labels. Search is not case-sensitive. Providing multiple search terms brings up devices and services that match at least one of the terms. See Page Level Search, on page 103.
- Filter for a device or template filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. See Filters.

Changing a Device's IP Address in Security Cloud Control

When you onboard an device to Security Cloud Control using an IP address, Security Cloud Control stores that IP address in its database and communicates with the device using that IP address. If the IP address of

the device changes, you can update the IP address stored in Security Cloud Control to match the new address. Changing the device's IP address on Security Cloud Control does not change device's configuration.

To change the IP address, Security Cloud Control uses to communicate with a device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**

Step 2 Click the **Devices** tab to locate the device.

Step 3 Click the appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required device.

Step 4 Select the device whose IP address it is you want to change.

Step 5 Above the **Device Details** pane, click the edit button next to the device's IP address.

Step 6 Enter the new IP address in the field and click the blue check button.

No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

Related Information:

- Moving Devices Between Tenants, on page 100
- Bulk Reconnect Devices to Security Cloud Control, on page 99

Changing a Device's Name in Security Cloud Control

All devices, models, templates, and services are given a name when they are onboarded or created in Security Cloud Control. You can change that name without changing the configuration of the device itself.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Device** tab to locate the device.

Step 3 Select the device whose name it is you want to change.

Step 4 Above the **Device Details** pane, click the edit button next to the device's name.

Step 5 Enter the new name in the field and click the blue check button.

No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

Export a List of Devices and Services

This article explains how to export your list of devices and services to a comma-separated value (.csv) file. Once in that format, you can open the file in a spreadsheet application such as Microsoft Excel to sort and filter the items in your list.

The export button is available in the devices and the templates tab. You are also allowed to export details from devices under the selected device type tab.

Before you export your list of devices and services, look at the filter pane and determine if the Inventory table is displaying the information you want to export. Clear all your filters to see all of your managed devices and services, or filter the information to display a subset of all your devices and services. The export function exports what you can see in the Inventory table.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab to export details from devices under that tab or click **All** to export details from all devices.

You can use the Filters and Page Level Search functionalities to find the required device.

Step 4 Click **Export list to CSV**:

Step 5 If prompted, save the .csv file.

Step 6 Open the .csv file in a spreadsheet application to sort and filter the results.

Export Device Configuration

You can only export one device configuration at a time. Use the following procedure to export a device's configuration to a JSON file:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required device.

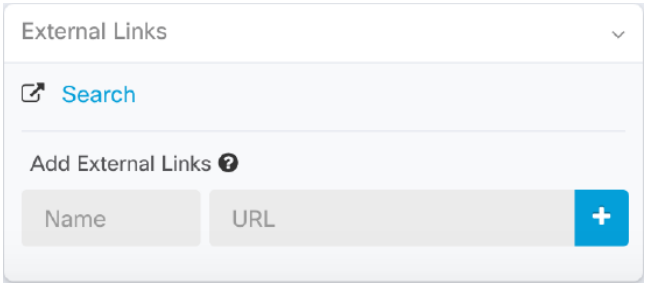
Step 4 Select the device you want so it is highlighted.

Step 5 In the **Actions** pane, select **Export Configuration**.

Step 6 Select **Confirm** to save the configuration as a JSON file.

External Links for Devices

You can create a hyperlink to an external resource and associate it with a device you manage with Security Cloud Control. You could use this feature to create a convenient link to the local manager of one of your devices (Firepower Device Manager (FDM) for an FTD). You could also use it to link to a search engine, documentation resource, a corporate wiki, or any other URL that you choose. You can associate as many external links with a device as you want. You can also associate the same link with multiple devices at the same time.



The links you create can reach anywhere, but your company's security requirements do not change. For example, if you ordinarily need to be connected to your corporate network, by being on-premises or through a VPN connection to reach a particular URL, those requirements remain. If your company blocks specific URLs, those URLs continue to be blocked. URLs that are not restricted continue to not be restricted.

Location Variable

We have created the {location} variable that you can incorporate in your URLs. This variable will be populated with the IP address of your device. For example,

```
https://{location}
```

or the FDM of your FDM-managed device.

Related Information:

- Write a Device Note, on page 100
- Export a List of Devices and Services, on page 95

Create an External Link from your Device

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select a device or model.

You can use the Filters and Page Level Search functionalities to find the required device.

Step 5 In the details pane, on the right, go to the **External Links** section.

Step 6 Enter a name for the link.

Step 7 Enter the URL for the link in the URL field. You need to specify the full URL, for example, for Cisco enter http://www.cisco.com.

Step 8 Click + to associate the link with the device.

Create an External Link to FDM

Here is a convenient way to open the Firepower Device Manager (FDM) of your FDM-managed device, directly from Security Cloud Control.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required device.

Step 4 Select a device or model.

Step 5 In the details pane, on the right, go to the **External Links** section.

Step 6 Enter a name for the link such as FDM.

Step 7 Enter https://{location} in the URL field. The {location} variable will be populated with the IP address of your device.

Step 8 Click the + box.

Create an External Link for Multiple Devices

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required devices.

Step 4 Select multiple devices or models.

Step 5 In the details pane, on the right, go to the **External Links** section.

Step 6 Enter a name for the link.

Step 7 Enter the URL you want to reach using one of these methods:

- Enter

  ```
  https://{location}
  ```

  in the URL field. The {location} variable will be populated with the IP address of your device. This creates an automatic link to the ASDM for your device.

- Enter the URL for the link in the URL field. You need to specify the full URL, for example, for Cisco enter http://www.cisco.com.

Step 8 Click + to associate the link with the device.

Edit or Delete External Links

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required device.

Step 4 Select a device or model.

Step 5 In the details pane, on the right, go to the **External Links** section.

Step 6 Mouse-over the name of the link to reveal the edit and delete icons.

Step 7 Click the appropriate icon to edit or delete the external link and confirm your action.

Edit or Delete External Links for Multiple Devices

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required devices.

Step 4 Select multiple devices or models.

Step 5 In the details pane, on the right, go to the **External Links** section.

Step 6 Mouse-over the name of the link to reveal the edit and delete icons.

Step 7 Click the appropriate icon to edit or delete the external link and confirm your action.

Bulk Reconnect Devices to Security Cloud Control

Security Cloud Control allows an administrator to attempt to reconnect more than one managed device to Security Cloud Control at the same time. When a device Security Cloud Control manages is marked "unreachable," Security Cloud Control can no longer detect out of band configuration changes or manage the device. There could be many different reasons for the disconnect. Attempting to reconnect the devices is a simple first step in restoring Security Cloud Control's management of the device.

Note If you are reconnecting devices having new certificates, Security Cloud Control automatically reviews and accepts the new certificates on the devices and continues to reconnect with them. However, if you are reconnecting with only one device, Security Cloud Control prompts you to review and accept the certificate manually to continue to reconnect with it.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate devices.

Step 3 Click the appropriate device type tab.

Use the Filters to look for devices whose connectivity status is "unreachable."

Step 4 From the filtered results, select the devices you want to attempt to reconnect.

Step 5 Click **Reconnect** . Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Look at the **notifications** tab for the progress of the bulk device reconnect action. If you want more information about how the actions in the bulk device reconnect job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control, on page 597.

Tip If a reconnect failure was caused because the device's certificate or credentials have changed, you will have to reconnect to those devices individually to add the new credentials and accept the new certificate.

Moving Devices Between Tenants

Once you have onboarded devices to a Security Cloud Control tenant, you cannot migrate the devices from one Security Cloud Control tenant to another. If you want to move your devices to a new tenant, you need to remove the devices from the old tenant and re-onboard them to the new tenant.

Device Certificate Expiry Detection

The management certificate is used for accessing FDM-managed and ASA devices from Security Cloud Control, while the Cisco Secure Client (formerly AnyConnect) is necessary for using virtual private network features on ASA, FDM-managed, and FTD devices from Security Cloud Control.

Security Cloud Control actively monitors the expiration status of these certificates and notifies the user when these certificates are nearing their expiration date or have expired. This prevents any disruptions in device operations due to certificate expiry. You should renew the corresponding certificate to address this issue.

The management certificate expiry check applies to ASA and FDM-managed devices, while the Secure Client certificate expiry check applies to ASA, FDM-managed, and FTD devices.

View Certificate Expiry Notification

In the top right corner, click the **Notifications** () icon to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The **High Priority** section displays the certificate expiration notifications.

These notifications are sent 30, 14, and 7 days before the certificate expiration date and then every day thereafter until the certificate either expires or is renewed with a valid certificate. You can also subscribe to receive these notifications by email on the **Notification Settings** section of the user preferences page. For more information, see User Notification Preferences.

Write a Device Note

Use this procedure to create a single, plain-text, note file for a device.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or model you want to create a note for.

Step 5 In the **Management** pane on the right, click **Notes**. Notes.

Step 6 Click the editor button on the right and select the Default text editor, Vim, or Emacs text editors.

Step 7 Edit the Notes page.

Step 8 Click **Save**.
The note is saved in the tab.

Security Cloud Control Inventory Information

The **Inventory** page shows all physical and virtual onboarded devices and templates created from the onboarded devices. The page classifies devices and templates based on their type and displays them in the corresponding tabs dedicated to each device type. You can use Page Level Search functionality or apply a Filters to find devices within the selected device type tab.

You can view the following details on this page:

- The **Devices** tab shows all the live devices that are onboarded to Security Cloud Control.
- The **Templates** shows all the template devices created from live devices or configuration files imported to Security Cloud Control.

Security Cloud Control Labels and Filtering

Labels are used for grouping devices or objects. You can apply labels to one or more devices during onboarding or at any time after onboarding. You can apply labels to objects after you create them. Once you have applied labels to devices or objects, you can filter the contents of the device table or objects table by that label.

Note A label applied to a device is not extended to its associated objects, and a label applied to a shared object is not extended to its associated objects.

You can create a label group by using the following syntax “group name:label”. For example, Region:East or Region:West. If you were to create these two labels, the group label would be Region and you could choose from East or West in that group.

Applying Labels to Devices and Objects

To apply a label to devices, perform the following steps:

Procedure

Step 1 In the left pane, click **Security Devices** to add a label to a device.

Step 2 In the left pane, click **Objects** to add a label to an object.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select one or more devices or model in the generated table.

Step 6 In the **Add Groups and Labels** field on the right, specify a label for the device.

Step 7 Click blue + icon.

Filters

You can use many different filters on the **Inventory** and **Objects** pages to find the devices and objects you are looking for.

To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

Note When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.

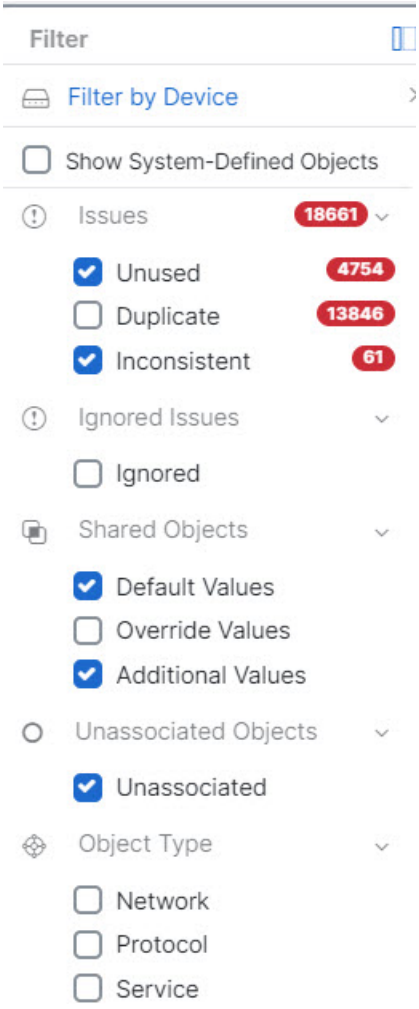
- FDM: Devices managed using FTD API or FDM.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

The object type filter allows you to filter objects by type, such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter allows filtering objects having default values or override values.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values.



Use Security Cloud Control Search Functionality

The Security Cloud Control platform has a highly efficient search function that makes it easy to find anything you need. The search bar on each page is tailored to the content of that page, while the global search allows for a comprehensive search across the entire tenant. This saves time and effort, as you can quickly locate the necessary information.

Page Level Search

The page-level search enables you to search specific items on the Inventory, Policies, Objects, VPN, Change Log, and Jobs pages.

- In the **Inventory** space, you can simply start typing in the search bar, and devices that fit the search criteria will be displayed. You can type any partial part name of the device, IP address, or the serial number of the physical device to find the device.
- In the **Policies** space, you can search policies by their name, components or objects used in them.

- In the **Objects** space, you can search for an object by typing any partial part of the name of the object, or partial IP Address, port, or protocols.
- In the **VPN** space, you can search by tunnel name, device name, and IP address used in the VPN policies.
- In the **Change log** space, you can search logs based on events, device names, or actions.

Procedure

Step 1 Navigate to the search bar near the top of the interface.

Step 2 Type the search criteria into the Search Bar and the corresponding results will be displayed.

Global Search

The global search feature allows you to quickly locate and navigate to devices managed by Security Cloud Control.

All search results are based on the indexing option you choose. The indexing options are as follows:

- Full Indexing—Requires that you invoke the full indexing process. This process scans all the devices and objects in the system and displays them in the search index only after you invoke the indexing. To invoke full indexing, you must have administrative privileges.

  For more information, see Initiate Full Indexing, on page 105.

- Incremental Indexing—An event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.

The information that you enter in the search field is not case-sensitive. You can perform a global search using the following entities:

- Device Name—Supports partial device names, URL, IP address or range.
- Object Types—Supports object name, object descriptions, and configured values.
- Policy Types—Supports policy name, policy description, rule name, and rule comments.

  Cloud-delivered Firewall Management Center and On-Prem FMC managed in Security Cloud Control support the following policy types:

  - Access Control Policy
  - Prefilter Policy
  - Threat Defense NAT Policy

When you type a search expression, the interface begins to display search results and you do not need to press *Enter* to execute a search.

The search results display all devices and objects that match your search strings. If your search string matches more than device or object, the results appear under categories (devices, objects, and connected_fmc).

By default, the first item in the search result is highlighted and the related information for that item appears in the right pane. You can scroll through the search results and click any item to view the corresponding information. You can click the arrow icon besides the item to navigate to the corresponding page.

Note

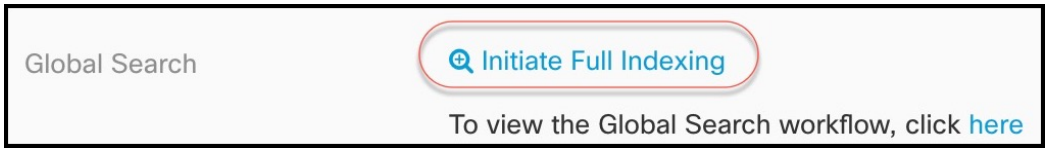
- Global search does not display duplicate search results. For objects, the UID of the shared object is used to navigate to the Object view.
- If you delete a device from Security Cloud Control, all associated objects are removed from the global search index.
- If you delete an object from the policy and retain the device before you initiate full indexing, the object remains in the global search index because it is associated with the device.

Initiate Full Indexing

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 In Global Search, click **Initiate Full Indexing** to trigger indexing.



Note Initiating full indexing clears existing indexing of the Security Cloud Control tenant.

Step 3 Click **here** to view the global search workflow.

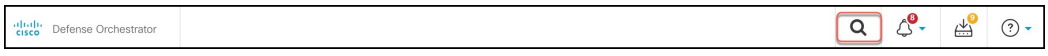
Perform a Global Search

Procedure

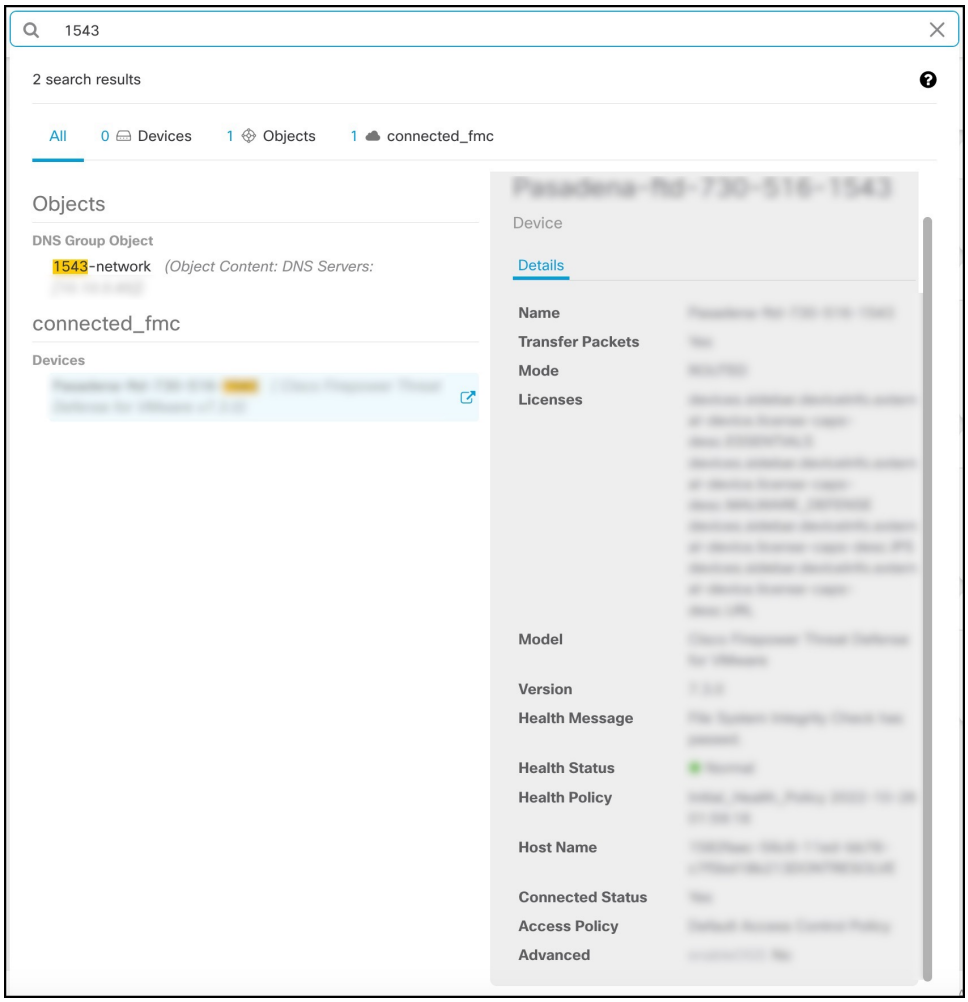
Step 1 Log into Security Cloud Control.

Step 2 Click the search icon in the top-right corner of the Security Cloud Control page and enter the search strings in the search field that appears.

Alternatively, you can press and hold the **Ctrl** key and the / key simultaneously on Windows, or the **Command** key and / key on Mac, to open the search bar.



The search results display a list of possible items as you begin entering the search strings. The search results appear under four categories: All, Devices, Objects, Policies, and Cloud-delivered Firewall Management Center. The right pane displays information for a selected search result.



Step 3 From the search result, select a device or an object, and click the arrow icon to navigate from the search results to the corresponding device and object page. From the search result, select an item, and click the arrow icon to navigate from the search results to the corresponding page.

Note Selecting a search result for devices in the cloud-delivered Firewall Management Center, allows you to navigate to the cloud-delivered Firewall Management Center user interface within Security Cloud Control.

For information on cloud-delivered Firewall Management Center, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control.

Step 4 Click **X** to close the search bar.

Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, Security Cloud Control recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

Security Cloud Control calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon:
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy. Before 28 June 2024, when you use an unassociated object in a rule or policy, Security Cloud Control created a copy of it and used the copy. Because of this behavior, you might have observed that there were two instances of the same object in the **Objects** menu. However, Security Cloud Control does not do that anymore. You can use an unassociated object in a rule or a policy but there are no duplicate objects that Security Cloud Control creates.

You can view the objects managed by Security Cloud Control by navigating to the **Objects** menu or by viewing them in the details of a network policy.

Security Cloud Control allows you to manage network and service objects across supported devices from one location. With Security Cloud Control, you can manage objects in these ways:

- Search for and Object Filters based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.

- Capture objects in use by a device after it has been on-boarded to Security Cloud Control.

Note Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes on devices, see Out-of-Band Changes on Devices, on page 575.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Security Cloud Control, on page 744 for more information.

Object Types

The following table describes the objects that you can create for your devices and manage using Security Cloud Control.

Table 2: Common Objects

Object Type	Description
Network	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
URL	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

Table 3: FDM-Managed Device Object Types

Object	Description
Application Filter Objects	An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.
Upload RA VPN AnyConnect Client Profile	AnyConnect Client Profile objects are file objects and represent files used in configurations, typically for remote access VPN policies. They can contain an AnyConnect Client Profile and AnyConnect Client Image files.
Certificate Objects	Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

Object	Description
DNS Group Objects	DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.
Create and Edit a Firepower Geolocation Filter Object	A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses.
Create or Edit an IKEv1 Policy	An IKEv1 policy object contain the parameters required for IKEv1 policies when defining VPN connections.
IKEv2 Policy	An IKEv2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections.
IKEv1 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 1 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
IKEv2 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
Network Objects	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
Security Zone Object	A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic.
Service Objects	Service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the TCP/IP protocol suite.
Create an SGT Group	A SGT dynamic object identifies source or destination addresses based on an SGT assigned by ISE and can then be matched against incoming traffic.
Syslog Server Objects	A syslog server object identifies a server that can receive connection-oriented or diagnostic system log (syslog) messages.

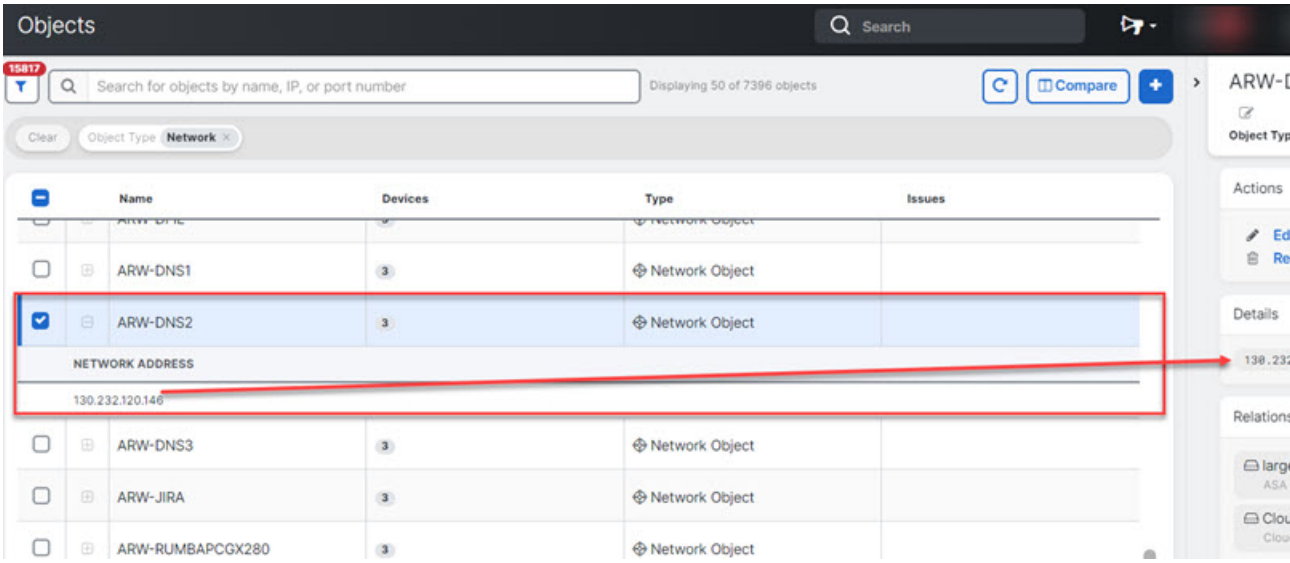
Object	Description
URL Objects	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

Shared Objects

Security Cloud Control calls objects on multiple devices with the same name and same contents, **shared objects**. Shared objects are identified by this icon

on the **Objects** page. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

When looking at a shared object, Security Cloud Control shows you the contents of the object in the object table. Shared objects have exactly the same contents. Security Cloud Control shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.



Object Overrides

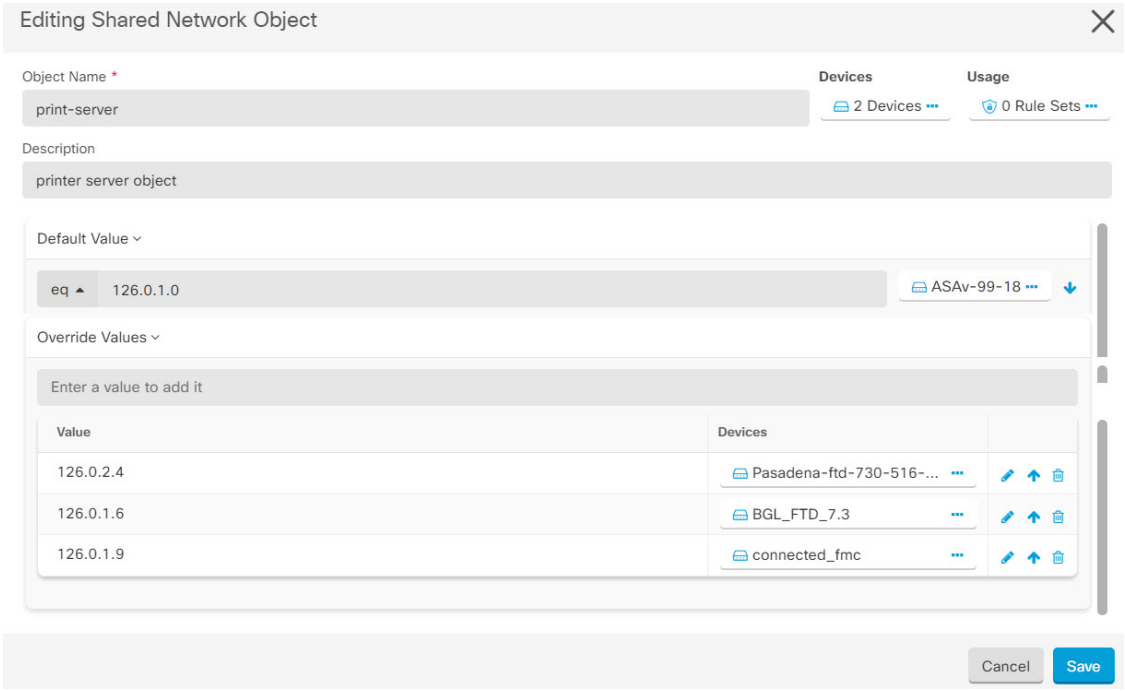
An object override allows you to override the value of a shared network object on specific devices. Security Cloud Control uses the corresponding value for the devices that you specify when configuring the override. Although the objects are on two or more devices with the same name but different values, Security Cloud Control doesn't identify them as **Inconsistent objects** only because these values are added as overrides.

You can create an object whose definition works for most devices, and then use overrides to specify modifications to the object for the few devices that need different definitions. You can also create an object

that needs to be overridden for all devices, but its use allows you to create a single policy for all devices. Object overrides allow you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices.

For example, consider a scenario where you have a printer server in each of your offices, and you have created a printer server object `print-server`. You have a rule in your ACL to deny printer servers from accessing the internet. The printer server object has a default value that you want to change from one office to another. You can do this by using object overrides and maintain rule and "printer-server" object consistent across all locations, although their values may be different.

Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes, see Out-of-Band Changes on Devices, on page 575.



Note Security Cloud Control allows you to override objects associated with the rules in a ruleset. When you add a new object to a rule, you can override it only after you attach a device to the ruleset and save the changes. See Configure Rulesets for a Device for more information.

Note If there are inconsistent objects, you can combine them into a single shared object with overrides. For more information, see Resolve Inconsistent Object Issues, on page 751.

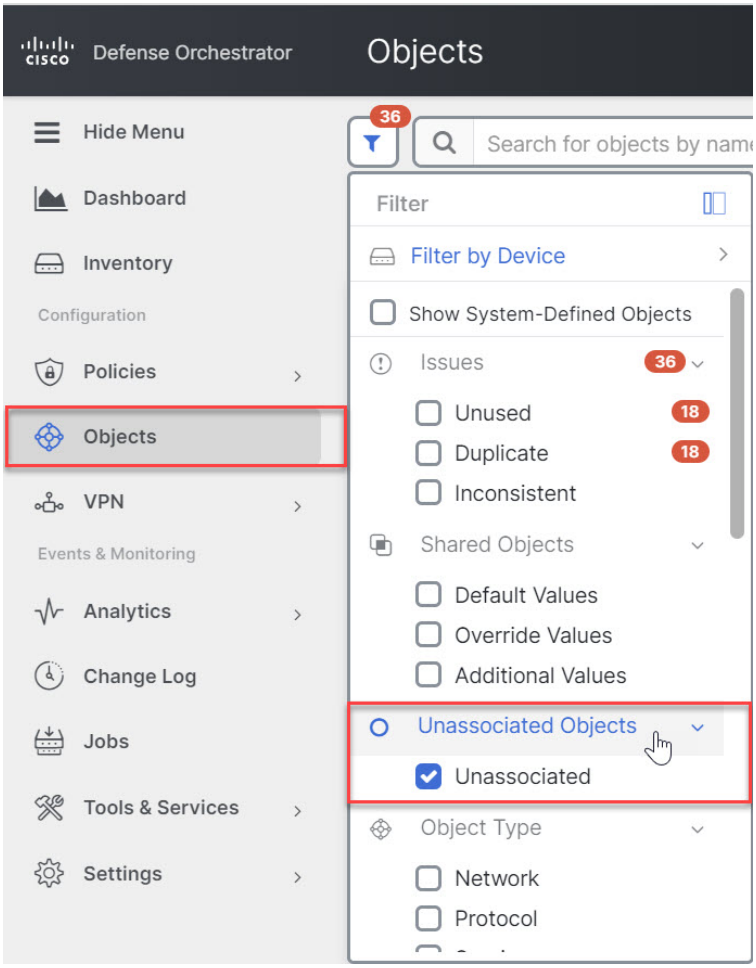
Unassociated Objects

You can create objects for immediate use in rules or policies. You can also create an object that is unassociated with any rule or policy. When you use that unassociated object in a rule or policy, Security Cloud Control

creates a copy of it and uses the copy. The original unassociated object remains among the list of available objects until it is either deleted by a nightly maintenance job, or you delete it.

Unassociated objects remain in Security Cloud Control as a copy to ensure that not all configurations are lost if the rule or policy associated with the object is deleted accidentally.

To view unassociated objects click in the left-hand pane of the Objects tab and check the **Unassociated** checkbox.



Compare Objects

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Filter the objects on the page to find the objects you want to compare.

Step 3 Click the **Compare** button Compare.

Step 4 Select up to three objects to compare.

Step 5 View the objects, side-by-side, at the bottom of the screen.

- Click the up and down arrows in the Object Details title bar to see more or less of the Object Details.
- Expand or collapse the Details and Relationships boxes to see more or less information.

Step 6 (Optional) The Relationships box shows how an object is used. It may be associated with a device or a policy. If the object is associated with a device, you can click the device name and then click **View Configuration** to see the configuration of the device. Security Cloud Control shows you the device's configuration file and highlights the entry for that object.

Filters

You can use many different filters on the **Inventory** and **Objects** pages to find the devices and objects you are looking for.

To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

Note When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.

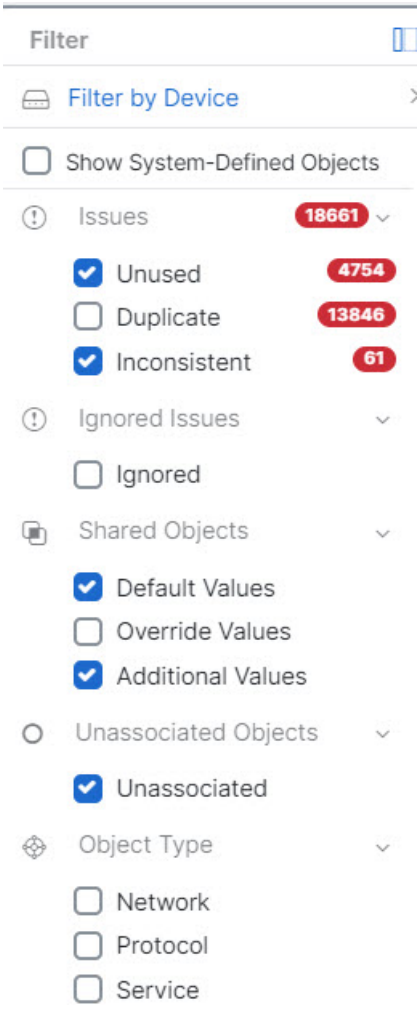
- FDM: Devices managed using FTD API or FDM.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

The object type filter allows you to filter objects by type, such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter allows filtering objects having default values or override values.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values.



Object Filters

To filter, click in the left-hand pane of the Objects tab:

- **Filter by Device**: Lets you pick a specific device so that you can see objects found on the selected device.
- **Issues**: Lets you pick unused, duplicate, and inconsistent objects to view.
- **Ignored Issues**: Lets you view all the objects whose inconsistencies you had ignored.
- **Shared Objects**: Lets you view all the objects that Security Cloud Control has found to be shared on more than one device. You can choose to see shared objects with only default values or override values, or both.
- **Unassociated Objects**: Lets you view all the objects that are not associated with any rule or policy.
- **Object Type**: Lets you select an object type to see only those type of objects that you have selected, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

Sub filters – Within each main filter, there are sub-filters you can apply to further narrow down your selection. These sub-filters are based on Object Type – Network, Service, Protocol, etc.

The selected filters in this filter bar would return objects that match the following criteria:

***** Objects that are on one of two devices. (Click **Filter by Device** to specify the devices.) AND are

*** Inconsistent** objects AND are

*** Network** objects OR **Service** objects AND

***** Have the word "**group**" in their object naming convention

Because **Show System Objects** is checked, the result would include both system objects and user-defined objects.

Show System-Defined Objects Filter

Some devices come with pre-defined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

Show System-Defined Objects is **off** by default. To display system objects in the object table, check **Show System-Defined Objects** in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

If you hide system objects, they will not be included in your search and filtering results. If you show system objects, they will be included in your object search and filtering results.

Configure Object Filters

You can filter on as few or as many criteria as you want. The more categories you filter by, the fewer results you should expect.

Procedure

Step 1 In the left pane, click **Objects**.

Step 2 Open the filter panel by clicking the filter icon at the top of the page. Uncheck any filters that have been checked to make sure no objects are inadvertently filtered out. Additionally, look at the search field and delete any text that may have been entered in the search field.

Step 3 If you want to restrict your results to those found on particular devices:

a. Click **Filter By Device**.

b. Search all the devices or click a device tab to search for only devices of a certain kind.

c. Check the device you want to include in your filter criteria.

d. Click **OK**.

Step 4 Check **Show System Objects** to include system objects in your search results. Uncheck **Show System Objects** to exclude system objects from your search results.

Step 5 Check the object **Issues** you want to filter by. If you check more than one issue, objects in any of the categories you check are included in your filter results.

Step 6 Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.

Step 7 Check the required filter in **Shared Objects** if you are filtering for objects shared between two or more devices.

- **Default Values**: Filters objects having only the default values.
- **Override Values**: Filters objects having overridden values.
- **Additional Values**: Filters objects having additional values.

Step 8 Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.

Step 9 Check the **Object Types** you want to filter by.

Step 10 You can also add an object name, IP address, or port number to the Objects search field to find objects with your search criteria among the filtered results.

When to Exclude a Device from Filter Criteria

When adding a device to filtering criteria, the results show you the objects on a device but not the relationships of those objects to other devices. For example, assume **ObjectA** is shared between ASA1 and ASA2. If you were to filter objects to find shared objects on ASA1, you would find **ObjectA** but the **Relationships** pane would only show you that the object is on ASA1.

To see all the devices to which an object is related, don't specify a device in your search criteria. Filter by the other criteria and add search criteria if you choose to. Select an object that Security Cloud Control identifies and then look in the Relationships pane. You will see all the devices and policies the object is related to.

Unignore Objects

One way to resolve unused, duplicate, or inconsistent objects is to ignore them. You may decide that though an object is Resolve an Unused Object Issue, a Resolve Duplicate Object Issues, or Resolve Inconsistent Object Issues, there are valid reasons for that state and you choose to leave the object issue unresolved. At some point in the future, you may want to resolve those ignored objects. As Security Cloud Control does not display ignored objects when you search for object issues, you will need to filter the object list for ignored objects and then act on the results.

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Object Filters.

Step 3 In the **Object** table, select the object you want to unignore. You can unignore one object at a time.

Step 4 Click **Unignore** in the details pane.

Step 5 Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

Deleting Objects

You can delete a single object or mulitple objects.

Delete a Single Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects**.

Step 2 Locate the object you want to delete by using object filters and the search field, and select it.

Step 3 Review the **Relationships** pane. If the object is used in a policy or in an object group, you cannot delete the object until you remove it from that policy or group.

Step 4 In the Actions pane, click the **Remove** icon .

Step 5 Confirm that you want to delete the object by clicking **OK**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Delete a Group of Unused Objects

As you onboard devices and start resolving object issues, you find many unused objects. You can delete up to 50 unused objects at a time.

Procedure

Step 1 Use the **Issues** filter to find **unused** objects. You can also use the Device filter to find objects that are not associated with a device by selecting **No Device**. Once you have filtered the object list, the object checkboxes appear.

Step 2 Check the **Select all** checkbox in the object table header to select all the objects found by the filter that appear in the object table; or, check individual checkboxes for individual objects you want to delete.

Step 3 In the Actions pane, click the **Remove** icon .

Step 4 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Network Objects

A network object can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. **Network groups** are collections of network objects and other individual addresses or subnetworks you add to the group. Network objects and network groups are used in access rules, network policies, and NAT rules. You can create, update, and delete network objects and network groups using Security Cloud Control.

Note that not all platforms support network objects, such as Cisco Merkai and Multicloud Defense; when you share dynamic objects, Security Cloud Control automatically translates the appropriate information from the originating platform or device into a set of usable information that Security Cloud Control can use.

Table 4: Pemitted Values of Network Objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Fully Qualified Domain Name	Subnet using CIDR Notation
FTD	IPv4 and IPv6	Yes	Yes	Yes	Yes
Multicloud Defense	IPv4 and IPv6	Yes	Yes	Yes	Yes

Table 5: Pemitted Contents of a Network Group

Device type	IP Value	Network Object	Network Groups
FTD	No	Yes	Yes
Multicloud Defense	Yes	Yes	Yes

Reusing Network Objects Across Products

If you have a Security Cloud Control tenant with a cloud-delivered Firewall Management Center and one or more on-premises management centers onboarded to your tenant:

- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object or group, a copy of the object is also added to the objects list on the **Objects > Other FTD Objects** page used when configuring cloud-delivered Firewall Management Center, and vice versa.
- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, or ASA network object or group, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the on-premises management center on which you want to use the object and discard the ones that you do not want. Navigate , **Administration** > **Firewall Management Center** select the on-premises management center, and click **Objects** to see your objects in the On-Premises Firewall Management Center user interface and assign them to policies.

Changes you make to network objects or groups on either page apply to the object or group instance on both pages. Deleting an object from one page also deletes the corresponding copy of the object from the other page.

Exceptions:

- If a network object of the same name already exists for cloud-delivered Firewall Management Center, the new Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object will not be replicated on the **Objects > Other FTD Objects** page of Security Cloud Control.
- Network objects and groups in onboarded threat defense devices that are managed by on-premises Secure Firewall Management Center are not replicated on the **Objects > Other FTD Objects** page and cannot be used in cloud-delivered Firewall Management Center.

  Note that for on-premises Secure Firewall Management Center instances that have been *migrated* to cloud-delivered Firewall Management Center, network objects and groups *are* replicated to the Security Cloud Control objects page if they are used in policies that were deployed to FTD devices.
- Sharing Network Objects between Security Cloud Control and cloud-delivered Firewall Management Center is automatically enabled on new tenants but must be requested for existing tenants. If your network objects are not being shared with cloud-delivered Firewall Management Center, How Security Cloud Control Customers Open a Support Ticket with TAC to have the features enabled on your tenant.
- Sharing network objects between Security Cloud Control and On-Premises Management Center is not automatically enabled on Security Cloud Control for new on-premises management centers onboarded to Security Cloud Control. If your network objects are not being shared with On-Premises Management Center, ensure **Discover & Manage Network Objects** toggle button is enabled for the on-premises management center in **Settings** or How Security Cloud Control Customers Open a Support Ticket with TAC to have the features enabled on your tenant.

Viewing Network Objects

Network objects you create using Security Cloud Control and those Security Cloud Control recognizes in an onboarded device's configuration are displayed on the Objects page. They are labeled with their object type. This allows you to filter by object type to quickly find the object you are looking for.

When you select a network object on the Objects page, you see the object's values in the Details pane. The Relationships pane shows you if the object is used in a policy and on what device the object is stored.

When you click on a network group you see the contents of that group. The network group is a conglomerate of all the values given to it by the network objects.

Related Information:

- Create or Edit a Firepower Network Object or Network Groups

Create or Edit a Firepower Network Object or Network Groups

A Firepower network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects and network groups that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

Firepower network objects and groups can be used by ASA, threat defense, FDM-managed, and Meraki devices. See Reusing Network Objects Across Products, on page 118.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Table 6: IP addresses that can be added to network objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Partially Qualified Domain Name (PQDN)	Subnet using CIDR Notation
Firepower	IPv4 / IPv6	Yes	Yes	Yes	Yes

Related Information:

- Create a Firepower Network Object, on page 120
- Edit a Firepower Network Object, on page 122
- Add Additional Values to a Shared Network Group, on page 125
- Edit Additional Values in a Shared Network Group, on page 127

Create a Firepower Network Object

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network object**.

Step 6 In the **Value** section:

- Select **eq** and enter a single IP address, a subnet address expressed in CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and enter an IP address range.

Note Do not set a host bit value. If you enter a host bit value other than 0, Security Cloud Control unsets it while creating the object, because the cloud-delivered Firewall Management Center only accepts IPv6 objects with host bits not set.

Step 7 Click **Add**.

Attention: The newly created network objects aren't associated with any FDM-managed device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters. For more information, see Configure Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create a Firepower Network Group

A **network group** can contain network objects and network groups. When you create a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects** > **FDM Objects** page, a copy of the object is automatically added to the **Objects** > **Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network group**.

Step 6 In the **Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.

Step 7 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 8 If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 9 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Note: You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.

Step 10 After adding the required objects, click **Save** to create a new network group.

Step 11 Preview and Deploy Configuration Changes for All Devices.

Edit a Firepower Network Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects** > **FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects** > **Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the network object and click the edit icon  in the **Actions** pane.

Step 4 Edit the values in the dialog box in the same fashion that you created them in "Create a Firepower Network Group".

Note Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit a Firepower Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the network group you want to edit by using object filters and search field.

Step 3 Select the network group and click the edit icon  in the **Actions** pane.

Step 4 Change the object name and description if needed.

Step 5 If you want to change the objects or network groups that are already added to the network group, perform the following steps:

a. Click the edit icon  appearing beside the object name or network group to modify them.

b. Click the checkmark to save your changes. **Note**: You can click the remove icon to delete the value from a network group.

Step 6 If you want to add new network objects or network groups to this network group, you have to perform the following steps:

a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, Security Cloud Control provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

b. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

c. If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.

- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 7 Click **Save**. Security Cloud Control displays the policies that will be affected by the change.

Step 8 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 9 Preview and Deploy Configuration Changes for All Devices.

Add an Object Override

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object to which you want to add an override, using object filters and search field.

Step 3 Select the network object and click the edit icon in the **Actions** pane.

Step 4 Enter the value in the **Override Values** dialog box and click **+ Add Value**.

Important The override you are adding must have the same type of value that the object contains. For example, to a network object, you can configure an override only with a network value and not a host value.

Step 5 Once you see that the value is added, click the cell in the **Devices** column in **Override Values**.

Step 6 Click **Add Devices**, and choose the device to which you want the override to be added. The device you select must contain the object to which you are adding the override.

Step 7 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 8 Click **Confirm** to finalize the addition of the override to the object and any devices affected by it.

Note You can add more than one override to an object. However, you must select a different device, which contains the object, each time you are adding an override.

Step 9 See Object Overrides, on page 110 to know more about object overrides and Edit Object Overrides , on page 125 to edit an existing override.

Edit Object Overrides

You can modify the value of an existing override as long as the object is present on the device.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object having override you want to edit by using object filters and search field.

Step 3 Select the object having override and click the edit icon in the Actions pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click on the cell in the **Devices** column in **Override Values** to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Override Values** to push and make it as the default value of the shared object.
- Click the delete icon next to the override you want to remove.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Add Additional Values to a Shared Network Group

The values in a shared network group that are present on all devices associated with it are called "default values". Security Cloud Control allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When Security Cloud Control deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory". These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

Note If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See Resolve Inconsistent Object Issues, on page 751 for more information.

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the shared network group you want to edit by using object filters and search field.

Step 3 Click the edit icon  in the **Actions** pane.

- The **Devices** field shows the devices the shared network group is present.
- The **Usage** field shows the rulesets associated with the shared network group.
- The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.

Step 4 In the **Additional Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.

Step 5 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 6 If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 7 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 8 In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.

Step 9 Select the devices that you want and click **OK**.

Step 10 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 11 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 12 Preview and Deploy Configuration Changes for All Devices.

Edit Additional Values in a Shared Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the object having the override you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
- Click arrow in **Override Values** to push and make it as default objects of the shared network group.
- Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the or **Objects > FDM Objects** page deletes the replicated network object or group from the **Objects > Other FTD Objects** page and vice-versa.

URL Objects

URL objects and URL groups are used by Firepower devices. Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies. A URL object defines a single URL or IP address, whereas a URL group defines more than one URL or IP address.

Before You Begin

When creating URL objects, keep the following points in mind:

- If you do not include a path (that is, there is no / character in the URL), the match is based on the server's hostname only. The hostname is considered a match if it comes after the :// separator, or after any dot in the hostname. For example, ign.com matches ign.com and www.ign.com, but it does not match verisign.com.
- If you include one or more / character, the entire URL string is used for a substring match, including the server name, path, and any query parameters. However, we recommend that you do not use manual URL filtering to block or allow individual web pages or parts of sites, as servers can be reorganized and pages moved to new paths. Substring matching can also lead to unexpected matches, where the string you include in the URL object also matches paths on unintended servers or strings within query parameters.
- The system disregards the encryption protocol (HTTP vs HTTPS). In other words, if you block a website, both HTTP and HTTPS traffic to that website is blocked, unless you use an application condition to target a specific protocol. When creating a URL object, you do not need to specify the protocol when creating an object. For example, use example.com rather than http://example.com.
- If you plan to use a URL object to match HTTPS traffic in an access control rule, create the object using the subject common name in the public key certificate used to encrypt the traffic. Also, the system disregards subdomains within the subject common name, so do not include subdomain information. For example, use example.com rather than www.example.com.

  However, please understand that the subject common name in the certificate might be completely unrelated to a web site's domain name. For example, the subject common name in the certificate for youtube.com is *.google.com (this of course might change at any time). You will get more consistent results if you use the SSL Decryption policy to decrypt HTTPS traffic so that URL filtering rules work on decrypted traffic.

Note URL objects will not match HTTPS traffic if the browser resumes a TLS session because the certificate information is no longer available. So even if you carefully configure the URL object, you might get inconsistent results for HTTPS connections.

Create or Edit an FDM-Managed URL Object

URL objects are reusable components that specify a URL or IP address.

To create a URL object, follow these steps:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **URL**.

Step 3 Enter an object name and description.

Step 4 Select **Create a URL object.**

Step 5 Enter the specific URL or IP address for your object.

Step 6 Click **Add**.

Create a Firepower URL Group

A URL group can be made up of one or more URL objects representing one or more URLs or IP addresses. The Firepower Device Manager and Firepower Management Center also refer to these objects as "URL Objects."

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **URL**.

Step 3 Enter an object name and description.

Step 4 Select **Create a URL group.**

Step 5 Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding URL objects to the URL group.

Edit a Firepower URL Object or URL Group

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the details pane, click  to edit.

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Application Filter Objects

Application filter objects are used by Firepower devices. An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.

Although you can specify individual applications, application filters simplify policy creation and administration. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

You can select applications and application filters directly in a policy without using application filter objects. However, an object is convenient if you want to create several policies for the same group of applications or filters. The system includes several pre-defined application filters, which you cannot edit or delete.

Note Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

Note When an FDM-managed device is onboarded to Security Cloud Control, it converts the application filters to application filter objects without altering the rule defined in Access Rule or SSL Decryption. Because of a configuration change, the device's configuration status is changed to 'Not Synced' and requires configuration deployment from Security Cloud Control. In general, FDM does not convert the application filters to application filter objects until you manually save the filters.

Related Information:

- Create and Edit a Firepower Application Filter Object
- Deleting Objects

Create and Edit a Firepower Application Filter Object

An application filter object allows you to target hand-picked applications or a group of applications identified by the filters. This application filter objects can be used in policies.

Create a Firepower Application Filter Object

To create an application filter object, follow this procedure:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

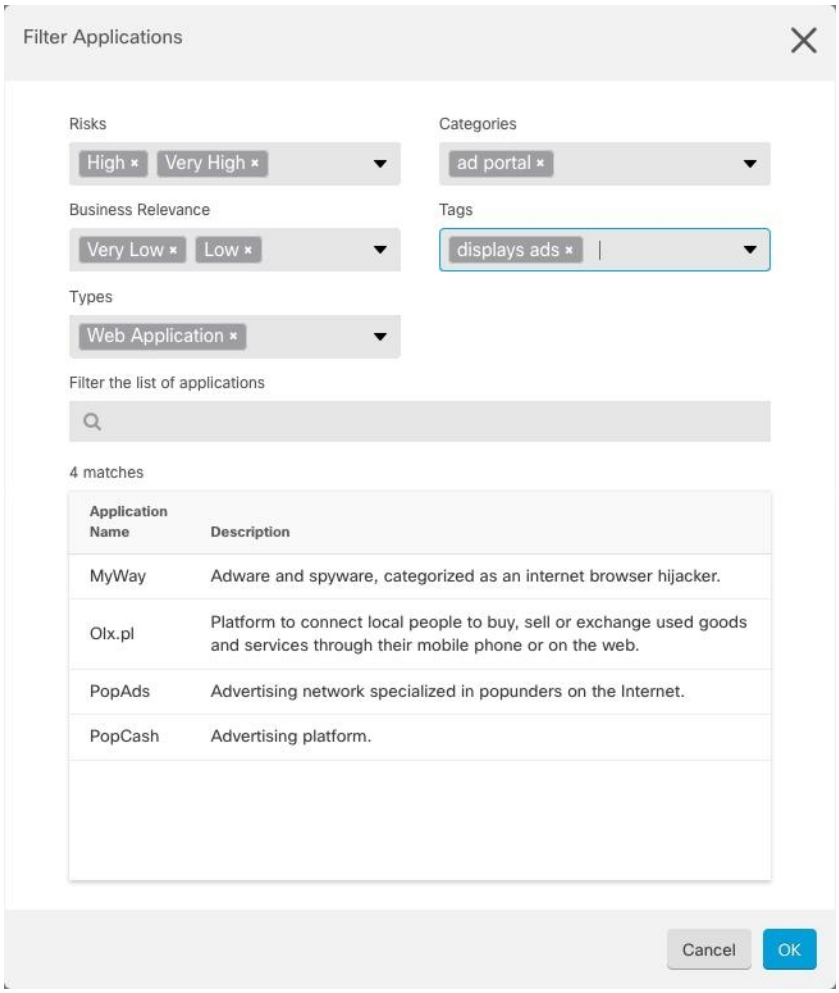
Step 2 Click **Create Object > FTD > Application Service**.

Step 3 Enter an **object name** for the object and optionally, a **description**.

Step 4 Click **Add Filter** and select the applications and filters to add to the object.

The initial list shows applications in a continually scrolling list. Click **Advanced Filter** to see the filter options and to get an easier view for selecting applications. Click **Add** when you have made your selections. You can repeat the process to add additional applications or filters.

Note Multiple selections within a single filter criteria have an OR relationship. For example, Risk is High OR Very High. The relationship between filters is AND, so Risk is High OR Very High, AND Business Relevance is Low OR Very Low. As you select filters, the list of applications in the display updates to show only those that meet the criteria. You can use these filters to help you find applications that you want to add individually, or to verify that you are selecting the desired filters to add to the rule.



Risks: The likelihood that the application is used for purposes that might be against your organization's security policy, from very low to very high.

Business Relevance: The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally, from very low to very high.

Types: The type of application.

- **Application Protocol:** Application protocols such as HTTP and SSH, which represent communications between hosts.

- **Client Protocol:** Clients such as web browsers and email clients, which represent software running on the host.
- **Web Application:** Web applications such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic.

Categories: A general classification for the application that describes its most essential function.

Tags: Additional information about the application, similar to category.

For encrypted traffic, the system can identify and filter traffic using only the applications tagged SSL Protocol. Applications without this tag can only be detected in unencrypted or decrypted traffic. Also, the system assigns the decrypted traffic tag to applications that the system can detect in decrypted traffic only, not encrypted or unencrypted.

Applications List (bottom of the display): This list updates as you select filters from the options above the list, so you can see the applications that currently match the filter. Use this list to verify that your filter is targeting the desired applications when you intend to add filter criteria to the rule. To add a specific application or applications to your object, select them from the filtered list. Once you select the applications, the filter will no longer apply. If you want the filter itself to be the object, do not select an application from the list. Then the object will represent ever application identified by the filter.

Step 5 Click **OK** to save your changes.

Edit a Firepower Application Filter Object

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon in the Actions pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 6 Click **Save**.

Step 7 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Related Information:

- Objects
- Object Filters
- Deleting Objects

Geolocation Objects

A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses. For example, using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

You can typically select geographical locations directly in a policy without using geolocation objects. However, an object is convenient if you want to create several policies for the same group of countries and continents.

Update Geolocation Database

To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB). At this time, this is not a task that you can perform using Security Cloud Control. See the following sections of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running to learn more about the GeoDB and how to update it.

- Updating System Databases and Feeds
- Updating System Databases

Create and Edit a Firepower Geolocation Filter Object

You can create a geolocation object by itself on the object page or when creating a security policy. This procedure creates a geolocation object from the object page.

To create a geolocation object, follow these steps:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **Geolocation**.

Step 3 Enter an **object name** for the object and optionally, a **description**.

Step 4 In the filter bar, start typing the name of a country or a region and you are presented with a list of possible matches.

Step 5 Check the country, countries, or regions that you want to add to the object.

Step 6 Click **Add**.

Edit a Geolocation Object

Procedure

Step 1 In the left pane, choose **Objects > FDM Objects**.

Step 2 Use the filter panes and search field to locate your object.

Step 3 In the **Actions** pane, click **Edit**.

Step 4 You can change the name of the object and add or remove countries and regions to your object.

Step 5 Click **Save**.

Step 6 You will be notified if any devices are impacted. Click **Confirm**.

Step 7 If a device or policy was impacted, open the **Inventory** page and **Preview and Deploy** the changes to the device.

DNS Group Objects

Domain Name System (DNS) groups define a list of DNS servers and some associated attributes. DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.

FDM-managed devices must have a DNS server configured prior to creating a new DNS Group Object. You can either add a DNS Server to theConfigure DNS Server in Security Cloud Control or create a DNS server in firewall device manager and then sync the FDM-managed configuration to Security Cloud Control. To create or modify the DNS server settings in firewall device manager, see **Configuring DNS for Data and Management Interfaces** in the Cisco Firepower Device Manager Configuration Guide, Version 6.4. or later.

Create a DNS Group Object

Use the following procedure to create a new DNS group object in Security Cloud Control:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **DNS Group**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Enter the IP address of a **DNS server**. You can add up to six DNS servers; click the **Add DNS Server**. If you want to remove a server address, click the delete icon.

Note The list is in priority order: the first server in the list is always used, and subsequent servers are used only if a response is not received from the servers above it. Although you can add up to six servers, only the first 3 servers listed will be used for the management interface.

Step 7 Enter the **Domain Search Name**. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

Step 8 Enter the amount of **Retries**. The number of times, from 0 to 10, to retry the list of DNS servers when the system does not receive a response. The default is 2. This setting applies to DNS groups used on the data interfaces only.

Step 9 Enter the **Timeout** value. The number of seconds, from 1 to 30, to wait before trying the next DNS server. The default is 2 seconds. Each time the system retries the list of servers, this timeout doubles. This setting applies to DNS groups used on the data interfaces only.

Step 10 Click **Add**.

Edit a DNS Group Object

You can edit a DNS group object that was created in Security Cloud Control or in firewall device manager. Use the following procedure to edit an existing DNS group object:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the **DNS Group Object** you want to edit by using object filters and search field.

Step 3 Select the object and click the edit icon in the **Actions** pane.

Step 4 Edit any of the following entries:

- Object Name.
- Description.
- DNS Server. You can edit, add, or remove DNS servers from this list.
- Domain Search Name.
- Retries.
- Timeout.

Step 5 Click **Save**.

Step 6 Preview and Deploy Configuration Changes for All Devices.

Delete a DNS Group Object

Use the following procedure to delete a DNS Group Object from Security Cloud Control:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the **DNS Group Object** you want to edit by using object filters and search field.

Step 3 Select the object and click the **Remove** icon.

Step 4 Confirm you want to delete the DNS group object and click **Ok**.

Step 5 Preview and Deploy Configuration Changes for All Devices.

Add a DNS Group Object as an FDM-Managed DNS Server

You can add a DNS group object as the preferred DNS Group for either the **Data Interface** or the **Management Interface**. See FDM-Managed Device Settings for more information.

Certificate Objects

Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

See the **About Certificates** and **Configuring Certificates** following sections of the Resuable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

About Certificates

Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

You can create the following types of certificate:

- **Internal certificates**—Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

  The system comes with the following pre-defined internal certificates, which you can use as is or replace: **DefaultInternalCertificate** and **DefaultWebServerCertificate**

- **Internal Certificate Authority (CA)** certificates—Internal CA certificates are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

  The system comes with the following pre-defined internal CA certificate, which you can use as is or replace: **NGFW-Default-InternalCA**

- **Trusted Certificate Authority (CA)** certificates—A trusted CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

  Certificate Authorities (CAs) are trusted authorities that "sign" certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization. CAs are responsible for managing certificate requests and issuing digital certificates.

  The system includes many trusted CA certificates from third party Certificate Authorities. These are used by SSL decryption policies for Decrypt Re-Sign actions.

For more information, see the **Certificate Types Used by Feature** section of the Reusable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Certificate Types Used by Feature

You need to create the right type of certificate for each feature. The following features require certificates.

Identity Policies (Captive Portal)—Internal Certificate

(Optional.) Captive portal is used in identity policies. Users must accept this certificate when authenticating to the device for purposes of identifying themselves and receiving the IP address associated with their usernames. If you do not supply a certificate, the device uses an automatically generated certificate.

SSL Decryption Policy—Internal, Internal CA, and Trusted CA Certificates.

(Required.) The SSL decryption policy uses certificates for the following purposes:

- Internal certificates are used for known key decryption rules.
- Internal CA certificates are used for decrypt re-sign rules when creating the session between the client and FDM-managed device.
- Trusted CA certificates
  - They are used indirectly for decrypt re-sign rules when creating the session between the FDM-managed device and server. Unlike the other certificates, you do not directly configure these certificates in the SSL decryption policy; they simply need to be uploaded to the system. The system includes a large number of trusted CA certificates, so you might not need to upload any additional certificates.
  - When creating an Active Directory Realm object and configuring the directory server to use encryption.

Configuring Certificates

Certificates used in identity policies or SSL decryption policies must be an X509 certificate in PEM or DER format. You can use OpenSSL to generate certificates if needed, obtain them from a trusted Certificate Authority, or create self-signed certificates.

Use these procedures to configure certificate objects:

- Uploading Internal and Internal CA Certificates
- Uploading Trusted CA Certificates
- Generating Self-Signed Internal and Internal CA Certificates
- To view or edit a certificate, click either the edit icon or the view icon for the certificate.
- To delete an unreferenced certificate, click the trash can icon (delete icon) for the certificate. See Deleting Objects.

Uploading Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

For information on the features that use these certificates, see Certificate Types Used by Feature.

Procedure

This procedure creates an internal or internal CA certificate by uploading a certificate file or pasting existing certificate text into a text box. If you want to generate a self signed certificate, see Generating Self-Signed Internal and Internal CA Certificates.

To create an internal or internal CA certificate object, or when adding a new certificate object to a policy, follow this procedure:

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:
  a. In the left pane, click **Objects > FDM Objects**.
  b. Click the plus button  and select **FTD** > **Certificate**
- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **Internal Certificate** or **Internal CA.**

Step 4 In step 2, select **Upload** to upload the certificate file.

Step 5 In step 3, in the **Server Certificate** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard. If you paste the certificate into the text box, the certificate must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

Step 6 In step 3, in the **Certificate Key** area, paste the key contents into the Certificate Key text box or upload the key file as explained in the wizard. If you paste the key into the text box, the key must include the BEGIN PRIVATE KEY or BEGIN RSA PRIVATE KEY and END PRIVATE KEY or END PRIVATE KEY lines.

Note The key cannot be encrypted.

Step 7 Click **Add**.

Uploading Trusted CA Certificates

A trusted Certificate Authority (CA) certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

For information on the features that use these certificates, see Certificate Types Used by Feature.

Obtain a trusted CA certificate from an external certificate authority, or create one using your own internal CA, for example, with OpenSSL tools. Then, use the following procedure to upload the certificate.

Procedure

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:
  a. In the left pane, click **Objects > FDM Objects**.
  b. Click the plus button and select **FTD** > **Certificate**.
- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **External CA Certificate** and click **Continue**. The wizard advances to step 3.

Step 4 In step 3, in the **Certificate Contents** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard.

The certificate must follow these guidelines:

- The name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.
- The certificate must be an X509 certificate in PEM or DER format.
- The certificate you paste must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
```

```
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

Step 5 Click **Add**.

Generating Self-Signed Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

You can also create these certificates using OpenSSL, or obtain them from a trusted CA, and upload them. For more information, see Uploading Internal and Internal CA Certificates.

For information on the features that use these certificates, see Certificate Types Used by Feature.

Note New self-signed certificates are generated with a 5-year validity term. Be sure to replace certificates before they expire.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Procedure

This procedure generates a self-signed certificate by entering the appropriate certificate field values in a wizard. If you want to create an internal or internal CA certificate by uploading a certificate file, see Uploading Internal and Internal CA Certificates.

To generate a self-signed certificate, follow this procedure:

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:

a. In the left pane, click **Objects > FDM Objects**.

b. Click the plus button and select **FTD** > **Certificate**.

- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **Internal Certificate** or **Internal CA.**

Step 4 In step 2, select **Self-Signed** to create the self-signed certificate in this step.

Step 5 Configure at least one of the following for the certificate subject and issuer information.

- Country (C)— Select the country code from the drop-down list.
- State or Province (ST)— The state or province to include in the certificate.
- Locality or City (L)— The locality to include in the certificate, such as the name of the city.
- Organization (O)— The organization or company name to include in the certificate.
- Organizational Unit (Department) (OU)— The name of the organization unit (for example, a department name) to include in the certificate.
- Common Name (CN)— The X.500 common name to include in the certificate. This could be the name of the device, web site, or another text string. This element is usually required for successful connections. For example, you must include a CN in the internal certificate used for remote access VPN.

Step 6 Click **Add**.

About IPsec Proposals

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.
- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

The following topics explain how to configure IPsec proposals for each IKE version:

- Managing an IKEv1 IPsec Proposal Object
- Managing an IKEv2 IPsec Proposal Object

Managing an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Security Cloud Control supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

Related Topics

Create an IKEv1 IPsec Proposal Object, on page 441

Create or Edit an IKEv1 IPsec Proposal Object

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button and select **FTD > IKEv1 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Select the Mode in which the IKEv1 IPsec Proposal object operates.

- **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Step 5 Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 422.

Step 6 Select the **ESP Hash** or integrity algorithm to use for authentication. For an explanation of the options, see Deciding Which Hash Algorithms to Use, on page 423.

Step 7 Click **Add**.

Managing an IKEv2 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

Related Topics

Create or Edit an IKEv2 IPsec Proposal Object, on page 442

Create or Edit an IKEv2 IPsec Proposal Object

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv2 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Configure the IKE2 IPsec proposal objects:

- **Encryption**—The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 422.
- **Integrity Hash**—The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use, on page 423.

Step 5 Click **Add**.

About Global IKE Policies

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

The following procedure explains how to configure the global policy through the Objects page. You can also enable, disable, and create policies when editing a VPN connection by clicking Edit for the IKE Policy settings.

The following topics explain how to configure IKE policies for each version:

- Managing IKEv1 Policies
- Managing IKEv2 Policies

Managing IKEv1 Policies

About IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of

IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv1 Policy, on page 437

Create or Edit an IKEv1 Policy

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv1 Policy** to create a new IKEv1 policy.
- In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv1 properties.

- **Priority**—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **Encryption**—The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group**—The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Lifetime**—The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

- **Authentication**—The method of authentication to use between the two peers. For more information, see Deciding Which Authentication Method to Use, on page 424.
  - **Preshared Key**—Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate**—Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer. The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.
- **Hash**—The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 422.

Step 5 Click **Add**.

Managing IKEv2 Policies

About IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv2 Policy, on page 439

Create or Edit an IKEv2 Policy

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv2 Policy** to create a new IKEv2 policy.
- In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv2 properties.

- **Priority**—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **State**—Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption**—The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 422.
- **Diffie-Hellman Group**—The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use, on page 424.
- **Integrity Hash**—The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 422.
- **Pseudo-Random Function (PRF) Hash**—The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 422.
- **Lifetime**—The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

Step 5 Click **Add**.

RA VPN Objects

Security Zone Object

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only.

The Firepower system creates the following zones during initial configuration and they are displayed in Security Cloud Control's object page. You can edit zones to add or remove interfaces, or you can delete the zones if you no longer use them.

- **inside_zone**-Includes the inside interface. This zone is intended to represent internal networks.
- **outside_zone**-Includes the outside interface. This zone is intended to represent networks external to your control, such as the internet.

Typically, you would group interfaces by the role they play in your network. For example, you would place the interface that connects to the internet in the **outside_zone** security zone, and all of the interfaces for your internal networks in the **inside_zone** security zone. Then, you could apply access control rules to traffic coming from the outside zone and going to the inside zone.

Before creating zones, consider the access rules and other policies you want to apply to your networks. For example, you do not need to put all internal interfaces into the same zone. If you have 4 internal networks, and you want to treat one differently than the other three, you can create two zones rather than one. If you have an interface that should allow outside access to a public web server, you might want to use a separate zone for the interface.

Related Information:

- Create or Edit a Firepower Security Zone Object
- Assign a Firepower Interface to a Security Zone
- Deleting Objects

Create or Edit a Firepower Security Zone Object

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only. For more information see,Security Zone Object.

A security zone object is not associated with a device unless it is used in a rule for that device.

Create a Security Zone Object

To create a security zone object, follow these instructions:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  and select **FTD** > **Security Zone** to create the object.

Step 3 Give the object a name and, optionally, a description.

Step 4 Select the interfaces to put in the security zone.

Step 5 Click **Add.**

Edit a Security Zone Object

After onboarding an FDM-managed device, you will find there are already at least two security zones, one is the inside_zone and the other is the outside_zone. These zones can be edited or deleted. To edit any security zone object, follow these instructions:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Find the object you want to edit:

- If you know the name of the object, you can search for it in the Objects page:
  - Filter the list by security zone.
  - Enter the name of the object in the search field.
  - Select the object.
- If you know the object is associated with a device, you can search for it starting on the **Inventory** page.
  - In the navigation pane, click **Inventory**.
  - Click the **Devices** tab.
  - Click the apporpriate tab.
  - Use the device Filters and Page Level Search bar to locate your device.
  - Select the device.
  - In the Management pane at the right, click  **Objects.**
  - Use the object filter and search bar to locate the object you are looking for.

Note If the security zone object you created is not associated with a rule in a policy for your device, it is considered "unassociated" and you will not see it among the search results for a device.

Step 3 Select the object.

Step 4 Click the **Edit** icon in the Actions pane at the right.

Step 5 After editing any of the attributes of the object. Click **Save**.

Step 6 After clicking Save you receive a message explaining how these changes will affect other devices. Click **Confirm** to save the changes or **Cancel**.

Service Objects

Firepower Service Objects

FTD service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the IP protocol suite.

FTD service groups are collections of service objects. A service group may contain objects for one or more protocols. You can use the objects and groups in security policies for purposes of defining network traffic matching criteria, for example, to use access rules to allow traffic to specific TCP ports. The system includes several pre-defined objects for common services. You can use these objects in your policies; however, you cannot edit or delete system-defined objects.

Firepower Device Manager and Firepower Management Center refer to service objects as port objects and service groups and port groups.

See Create and Edit Firepower Service Objects for more information.

Protocol Objects

Protocol objects are a type of service object that contain less-commonly used or legacy protocols. Protocol objects are identified by a name and protocol number. Security Cloud Control recognizes these objects in ASA and Firepower (FDM-managed device) configurations and gives them their own filter of "Protocols" so you can find them easily.

See Create and Edit Firepower Service Objects for more information.

ICMP Objects

An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. Security Cloud Control recognizes these objects in ASA and Firepower configurations when those devices are onboarded and Security Cloud Control gives them their own filter of "ICMP" so you can find the objects easily.

Using Security Cloud Control, you can rename or remove ICMP objects from an ASA configuration. You can use Security Cloud Control to create, update, and delete ICMP and ICMPv6 objects in a Firepower configuration.

Note For the ICMPv6 protocol, AWS does not support choosing specific arguments. Only rules that allow all ICMPv6 messages are supported.

See Create and Edit Firepower Service Objects for more information.

Related Information:

- Deleting Objects, on page 116

Create and Edit Firepower Service Objects

To create a firepower service object, follow these steps:

firewall device manager (FDM-managed) service objects are reusable components that specify a TCP/IP protocol and a port. The firewall device manager, On-Premises Firewall Management Center and Cloud-delivered Firewall Management Center refer to these objects as "Port Objects."

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue button  on the right to create an object, and select **FTD** > **Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service object.**

Step 5 Click the **Service Type** button and select the protocol for which you want to create an object.

Step 6 Configure the protocol as follows:

- **TCP**, **UDP**
  - Select **eq** and then enter either a port number or a protocol name. For example, you could enter 80 as a port number or HTTP as the protocol name.
  - You can also select **range** and then enter a range of port numbers, for example, **1 65535** (to cover all ports).
- **ICMP**, **IPv6-ICMP**-Select the ICMP **Type.** Select **Any** for the type to apply to all ICMP messages. For information on the types and codes, see the following pages:
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other**-Select the desired protocol.

Step 7 Click **Add**.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Create a Firepower Service Group

A service group can be made up of one or more service objects representing one or more protocols. The service objects need to be created before they can be added to the group. The Firepower Device Manager and Firepower Management Center refer to these objects as "Port Objects."

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue button  on the right to create an object, and select **FTD** > **Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service group.**

Step 5 Add an object to the group by clicking **Add Object.**

- Click **Create** to create a new object as you did above in Create and Edit Firepower Service Objects above.
- Click **Choose** to add an existing service object to the group. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding service objects to the service group.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Edit a Firepower Service Object or Service Group

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the Actions pane, click **Edit** .

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Security Group Tag Group

Security Group Tags

About Security Group Tags

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria. Thus, you can block or allow access based on security group membership rather than IP addresses.

In ISE, you can create a SGT and assign host or network IP addresses to each tag. If you assign an SGT to a user's account, the SGT is assigned to the user's traffic. After you configure FDM-managed device to connect to an ISE server and create the SGT, you can create SGT groups in Security Cloud Control and build access control rules around them. Note that you must configure ISE's SGT Exchange Protocol (SXP) mapping before you can associate an SGT to an FDM-managed device. See **Security Group Tag Exchange Protocol** in the Cisco Identity Services Engine Administrator Guide of the version you are currently running for more information.

When an FDM-managed device evaluates SGT as a traffic matching criteria for an access control rule, it uses the following priority:

1. The source SGT defined in the packet, if any. No destination matching is done using this technique. For the SGT to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
2. The SGT assigned to the user session, as downloaded from the ISE session directory. You need to enable the option to listen to session directory information for this kind of SGT matching, but this option is on by default when you first create the ISE identity source. The SGT can be matched to source or destination. Although not required, you would also normally set up a passive authentication identity rule, using the ISE identity source along with an AD realm, to collect user identity information.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is within the range for an SGT, then the traffic matches the access control rule that uses the SGT. The SGT can be matched to source or destination.

Note You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on a relevant collections of tags if that is appropriate.

Version Support

Security Cloud Control currently supports SGT and SGT groups on FDM-managed devices running Version 6.5 and later. an FDM-managed device allows you to configure and connect to an ISE server in Version 6.5 and later but not does not support SGT configuration in the UI until Version 6.7.

From the FDM-managed UI, this means that an FDM-managed device running Version 6.5 or later can download SXP mappings of SGTs but cannot be manually added to objects or access control rules. To make changes to the SGTs for devices running Version 6.5 or Version 6.6, you must use the ISE UI. If the device running Version 6.5 is onboarded to Security Cloud Control, however, you can see the current SGTs associated with the device and create SGT groups.

SGT in Security Cloud Control

Security Group Tags

SGTs are read-only in Security Cloud Control. You cannot create or edit an SGT in Security Cloud Control. To create an SGT, see the Cisco Identity Services Engine Administrator Guide of the version your are currently running.

SGT Groups

Note An FDM-managed device refers to groups of SGTs as SGT dynamic objects. In Security Cloud Control, these lists of tags are currently called SGT groups. You can create an SGT group in Security Cloud Control without referring to the FDM-managed device or ISE UI.

Use SGT groups to identify source or destination addresses based on an SGT assigned by ISE. You can then use the objects in access control rules for purposes of defining traffic matching criteria. You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information.

Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

In order to create an SGT group in Security Cloud Control, you must have at least one SGT already configured and SGT mappings from an ISE server configured for the FDM-managed console of the device you want to use. Note that if more than one FDM-managed device is associated with the same ISE server, an SGT or SGT group can be applied to more than one device. If a device is not associated with an ISE server, you cannot include SGT objects in your access control rule, or apply an SGT group to that device configuration.

SGT Groups in Rules

SGT groups can be added to access control rules; they appear as source or destination network objects. For more information about how networks work in rules, see Source and Destination Criteria in an FDM-Managed Access Control Rule.

You can create an SGT group from the Objects page. See Create an SGT Group, on page 154 for more information.

Create an SGT Group

To create an SGT group that can be used for an access control rule, use the following procedure:

Before you begin

You must have the following configurations or environments configured prior to creating a security group tag (SGT) group:

- FDM-managed device must be running at least Version 6.5.
- You must configure the ISE identity source to subscribe to SXP mappings and enable deploy changes. To manage SXP mappings, see **Configure Security Groups and SXP Publishing in ISE** of the Firepower Device Manager Configuration Guide for the version you're using, Version 6.7 and later.
- All SGTs must be created in ISE. To create an SGT, see the Cisco Identity Services Engine Configuration Guide of the version your are currently running.

Procedure

Step 1 On the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Click **SGT** and use the drop-down menu to check all the applicable SGTs you want included in the group. You can sort the list by SGT name.

Step 7 Click **Save**.

Note You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Edit an SGT Group

To edit an SGT group, use the following procedure:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the SGT group you want to edit by using object filters and search field.

Step 3 Select the SGT group and click the edit icon  in the **Actions** pane.

Step 4 Modify the SGT group. Edit the name, description, or the SGTs associated with the group.

Step 5 Click **Save**.

Note You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Add an SGT Group to an Access Control Rule

To add an SGT group to an access control rule, use the following procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to add the SGT group to.

Step 4 In the**Management** pane, select **Policy**.

Step 5 Click the blue plus button  for either the **Source** or **Destination** objects and select **SGT Groups**.

Step 6 Locate the SGT group(s) you want to edit by using object filters and search field.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices.

Note If you need to create an additional SGT group, click **Create New Object**. Fill in the required information mentioned in Create an SGT Group and **Add** the SGT group to the rule.

Syslog Server Objects

FDM-managed devices have a limited capacity to store events. To maximize storage for events, you can configure an external server. A system log (syslog) server object identifies a server that can receive connection-oriented or diagnostic syslog messages. If you have a syslog server set up for log collection and analysis, you can use the Security Cloud Control to create objects to define them and use the objects in the related policies.

Create and Edit Syslog Server Objects

To create a new syslog server object, follow these steps:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the **Create Object** button .

Step 3 Select **Syslog Server** under FDM-managed device object types

Step 4 Configure the syslog server object properties:

- **IP Address**—Enter the IP address of the syslog server.
- **Protocol Type**—Select the protocol that your syslog server uses to receive messages. If you select TCP, the system can recognize when the syslog server is not available, and stops sending events until the server is available again.
- **Port Number**—Enter a valid port number to use for syslog. If your syslog server uses default ports, enter 514 as the default UDP port or 1470 as the default TCP port. If the server does not use default ports, enter the correct port number. The port must be in the range 1025 to 65535.
- **Select an interface**—Select which interface should be used for sending diagnostic syslog messages. Connection and intrusion events always use the management interface. Your interface selection determines the IP address associated with syslog messages. Note that you can only select **one** of the options listed below. You cannot select both. Select one of the following options:
  - **Data Interface**—Use the data interface you select for diagnostic syslog messages. Select an interface from the generated list. If the server is accessible through a bridge group member interface, select the bridge group interface (BVI). If it is accessible through the Diagnostic interface (the physical management interface), we recommend that you select Management Interface instead of this option. You cannot select a passive interface. For connection and intrusion syslog messages, the source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

- **Management Interface**—Use the virtual management interface for all types of syslog messages. The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

Step 5 Click **Add**.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit Syslog Server Objects

To edit an existing syslog server object, follow these steps:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the desired syslog server object and select it. You can **filter** the object list by the syslog server object type.

Step 3 In the Actions pane, click **Edit**.

Step 4 Make the desired edits and click **Save**.

Step 5 Confirm the changes you made.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Deleting Objects

Create a Syslog Server Object for Secure Logging Analytics (SaaS)

Create a syslog server object with the IP address, TCP port, or UDP port of the Secure Event Connector (SEC) you want to send events to. You would create one syslog object for every SEC that you have onboarded to your tenant but you would only send events from one rule to one syslog object representing one SEC.

Prerequisite

This task is part of a larger workflow. See Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices, on page 614 before you begin.

Procedure

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the **Create Object** button  .

Step 3 Select **Syslog Server** under FDM-managed device object types.

Step 4 Configure the syslog server object properties. To find these properties of the SEC, from the navigation pane on the left, choose **Tools & Services** > **Secure Connectors**. Then select the Secure Event Connector you want to configure the syslog object for and look in the Details pane on the right.

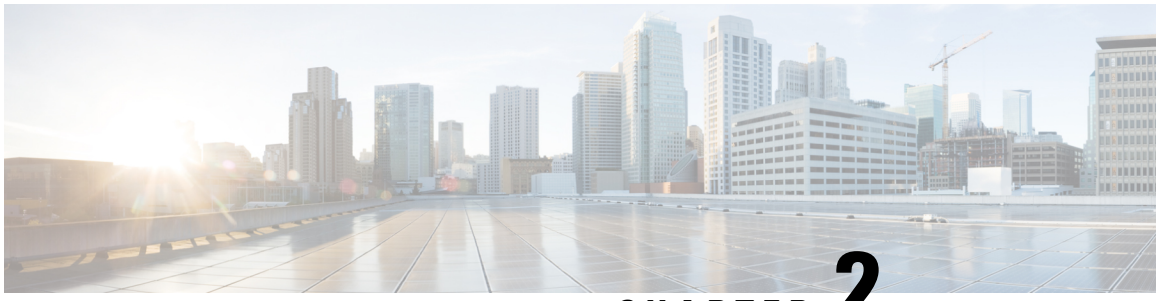
- **IP Address**—Enter the IP address of the SEC.
- **Protocol Type**—Select TCP or UDP.
- **Port Number**—Enter port 10125 if you selected TCP or 10025 if you selected UDP.
- **Select an interface**—Select the interface configured to reach the SEC.

Note FDM-managed device supports one syslog object per IP address so you will have to choose between using TCP and UDP.

Step 5 Click **Add**.

What to do next

Continue with Step 3 of Existing Security Cloud Control Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud.



CHAPTER 2

Onboard Devices and Services

You can onboard both live devices and model devices to Security Cloud Control. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control to the device or service.

See Secure Device Connector, on page 14 for more information on the SDC and its state.

This chapter covers the following sections:

Onboard a Threat Defense Device

Attention Secure Firewall device manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. Open a Support Ticket with TAC to enable this platform.

There are different methods of onboarding a threat defense device. We recommend using the registration key method.

If you experience issues while onboarding a device, see Troubleshoot FDM-Managed Device Onboarding Using Serial Number, on page 720 or Failed Because of Insufficient License , on page 716 for more information.

Onboard a Threat Defense Device to Cloud-delivered Firewall Management Center

You can onboard threat defense devices running version 7.2 and later to the Cloud-delivered Firewall Management Center. See Onboard an FTD to the Cloud-Delivered Firewall Management Center for more information.

Onboard a Threat Defense Device with a Serial Number

This procedure is a simplified method of onboarding the Firepower 1000, Firepower 2100, or Secure Firewall 3100 series physical devices running supported versions of software. To onboard the device, you need the chassis serial number or PCA serial number of the device and ensure that the device is added to a network that can reach the internet.

You can onboard new factory-shipped devices or already configured devices to Security Cloud Control.

See Onboard an FDM-Managed Device using the Device's Serial Number, on page 176 for more information.

Onboard a Threat Defense Device with a Registration Key

We recommend onboarding threat defense devices with a registration key. This is beneficial if your device is assigned an IP address using DHCP. If that IP address changes for some reason, your threat defense device remains connected to Security Cloud Control if you have onboarded it with a registration key.

- Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 168
- Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, on page 172

Onboard an Threat Defense Device Using Credentials

You can onboard a threat defense device using the device credentials and the IP address of the device's outside, inside, or management interface depending on how the device is configured in your network. To onboard a device with credentials, see Onboard an FDM-Managed Device Using Username, Password, and IP Address, on page 166. To onboard with an interface address, see Onboard a Threat Defense Device later in this article.

Security Cloud Control needs HTTPS access to the device in order to manage it. How you allow HTTPS access to the device depends on how your device is configured in your network and whether you onboard the device using a Secure Device Connector or a Cloud Connector.

Note If you connect to https://us.manage.security.cisco.com and you are using software version 6.4, you must onboard the threat defense device with this method. You cannot use the registration key method.

When using device credentials to connect Security Cloud Control to a device, it a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. The threat defense device, when onboarded with credentials, can be onboarded to Security Cloud Control using an SDC.

Note that customers also using the threat defense devie as the head-end for VPN connections will not be able to use the outside interface to manage their device.

Onboard a Threat Defense Cluster

You can onboard a threat defense device that is clustered prior to onboarding to Security Cloud Control. Clustering lets you group multiple firewall threat defense units together as a single logical device that provides the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

See Onboard a Clustered Secure Firewall Threat Defense Device, on page 191.

FDM-Managed Device Configuration Prerequisites for Onboarding

FDM-Managed Device Management

You can only onboard threat defense devices that are being managed by Secure Firewall device manager (FDM). threat defense devices being managed by Secure Firewall Management Center cannot be managed by the cloud-delivered Firewall Management Center.

If the device is not configured for local management, you must switch to local management before onboarding the device. See the **Switching Between Local and Remote Management** chapter of the Secure Firewall Threat Defense Configuration Guide for Firepower Device Manager.

Licensing

The device **must** have at least an license installed before it can be onboarded to Security Cloud Control although you can have a Smart License applied in some circumstances.

Onboarding Method	Secure Firewall device manager Software Version	90-day Evaluation licensed allowed?	Can the device already be smart-licensed before onboarding?	Can the device already be registered with Cisco Cloud Services before you onboarding?
Credentials (user name and password)	6.4 or later	Yes	Yes	Yes
Registration Key	6.4 or 6.5	Yes	No. Unregister the smart license and then onboard the device.	N/A
Registration Key	6.6 or later	Yes	Yes	No. Unregister the device from Cisco Cloud Services and then onboard the device.
Zero-Touch Provisioning	6.7 or later	Yes	Yes	Yes
Onboarding a device with a Serial Number	6.7 or later	Yes	Yes	Yes

See Cisco Firepower System Feature Licenses for more information.

Device Addressing

It is a best practice that the address you use to onboard the FDM-managed device is a static address. If the device's IP address is assigned by DHCP, it would be optimal to use a DDNS (dynamic domain name system) to automatically update your device's domain name entry with the new IP address of the device if it changes.

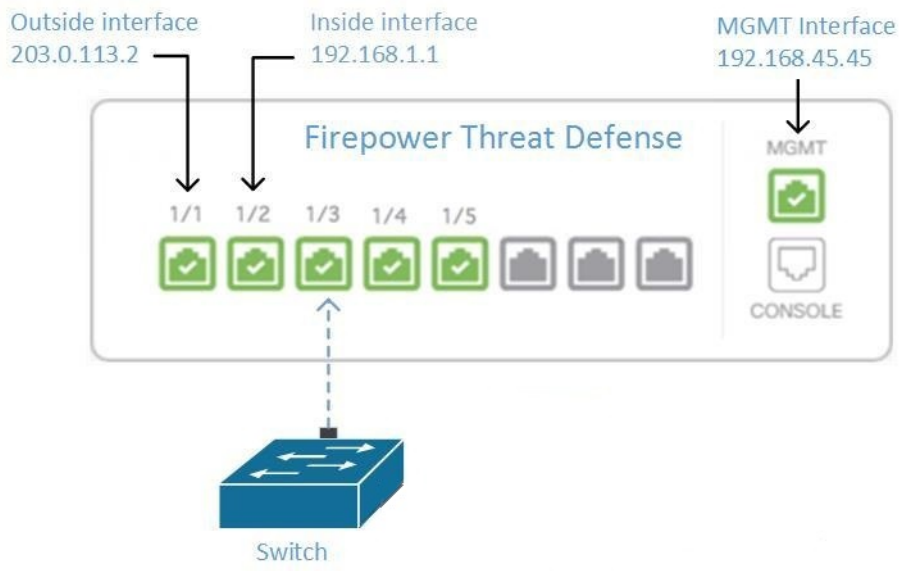
Note FDM-managed devices do not natively support DDNS; you must configure your own DDNS.

Important If your device gets an IP address from a DHCP server, and you *do not* have a DDNS server updating the FDM-managed device's domain name entry with any new IP addresses, or your device receives a new address, you can Changing a Device's IP Address in Security Cloud Control and then Bulk Reconnect Devices to Security Cloud Control. Better still, onboard the device with a registration key.

Managing an FDM-Managed Device from the Inside Interface

Managing an FDM-managed device using the inside interface may be desirable if the dedicated MGMT interface is assigned an address that is not routable within your organization; for example, it might only be reachable from within your data center or lab.

Figure 7: Interface Addresses



Remote Access VPN Requirement

If the FDM-managed device you manage with Security Cloud Control will be managing Remote Access VPN (RA VPN) connections, Security Cloud Control must manage the device using the inside interface.

What to do next:

Continue to Manage an FDM-Managed Device from the Inside Interface, on page 2 for the procedure for configuring the FDM-managed device.

Manage an FDM-Managed Device from the Inside Interface

This configuration method:

- Assumes that the FDM-managed device has not been on-boarded to Security Cloud Control.
- Configures a data interface as the inside interface.
- Configures the inside interface to receive MGMT traffic (HTTPS).
- Allows the address of the cloud connector to reach the inside interface of the device.

Before you begin

Review the prerequisites for this configuration in these topics:

- Managing an FDM-Managed Device from the Inside Interface, on page 2
- Connect Security Cloud Control to your Managed Devices, on page 15

Procedure

Step 1 Log in to the Secure Firewall device manager.

Step 2 In the **System Settings** menu, click **Management Access**.

Step 3 Click the **Data Interfaces** tab and click **Create Data Interface**.

a. In the **Interface** field, select the pre-named "**inside**" interface from the list of interfaces.

b. In the **Protocols** field, select **HTTPS** if it is not already.

c. In the **Allowed Networks** field, select the network objects that represent the networks inside your organization that will be allowed to access the inside address of the FDM-managed device. The IP address of the SDC or cloud connector should be among the addresses allowed to access the inside address of the device.

In the Interface Addresses diagram, the SDC's IP address, 192.168.1.10 should be able to reach 192.168.1.1.

Step 4 **Deploy the change**. You can now manage the device using the inside interface.

What to do next

What if you are using a Cloud Connector?

Use the procedure above and add these steps:

- Add a step to "NAT" the outside interface to (203.0.113.2) to the inside interface (192.168.1.1). See Interface Addresses.

- In step 3c of the procedure above, your "Allowed Network" is a network group object containing the public IP addresses of the cloud connector.
- Add a step that creates an Access Control rule allowing access to the outside interface (203.0.113.2) from the public IP addresses of the cloud connector. See for a list of all the Cloud Connector IP addresses for the various Security Cloud Control regions.

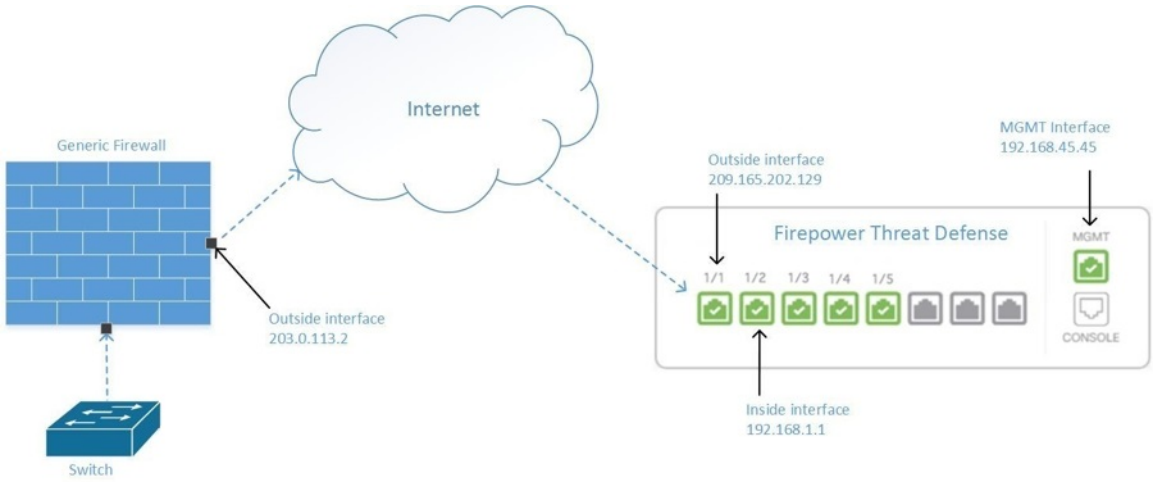
Onboard the FDM-Managed Device

The recommended way of onboarding the FDM-managed device to Security Cloud Control is to use the registration token onboarding approach. After you configure the inside interface to allow management access from the Cloud Connector to the FDM-managed device, onboard the FDM-managed device with the user name and password. See Onboard a Threat Defense Device for more information. You will connect using the IP address of the inside interface. In our scenario above, that address is 192.168.1.1.

Managing an FDM-Managed Device from the Outside Interface

Managing an cloud-delivered Firewall Management Center device from the outside interface may be desirable if you have one public IP address assigned to a branch office and Security Cloud Control is managed using a Cloud Connector at another location.

Figure 8: Device Management on Outside Interface



This configuration doesn't mean that the physical MGMT interface is no longer the device's management interface. If you were in the office where the cloud-delivered Firewall Management Center device was located, you would be able to connect to the address of the MGMT interface and manage the device directly.

Remote Access VPN Requirement

If the device you manage with cloud-delivered Firewall Management Center will be managing Remote Access VPN (RA VPN) connections, cloud-delivered Firewall Management Center will not be able to manage the cloud-delivered Firewall Management Center device using the outside interface. See Managing an FDM-Managed Device from the Inside Interface instead.

What to do next:

Continue to Manage the FDM-Managed Device's Outside Interface, on page 4 for the procedure for configuring the cloud-delivered Firewall Management Center device.

Manage the FDM-Managed Device's Outside Interface

This configuration method:

1. Assumes that the FDM-managed device has not been on-boarded to Security Cloud Control.
2. Configures a data interface as the outside interface.
3. Configures management access on the outside interface.
4. Allows the public IP address of the cloud connector (after it has been NAT'd through the firewall) to reach the outside interface.

Before you begin

Review the prerequisites for this configuration in these topics:

- Manage the FDM-Managed Device's Outside Interface, on page 4
- Connect Security Cloud Control to your Managed Devices, on page 15

Procedure

Step 1 Log in to the Secure Firewall device manager.

Step 2 In the **System Settings** menu, click **Management Access**.

Step 3 Click the **Data Interfaces** tab and click **Create Data Interface**.

a. In the **Interface** field, select the pre-named "**outside**" interface from the list of interfaces.

b. In the **Protocols** field, select **HTTPS** if it is not already. Security Cloud Control only needs HTTPS access.

c. In the **Allowed Networks** field, create a host network object containing the public-facing IP address of the cloud connector after it gets NAT'd through the firewall.

In the Device Management from Outside Interface network diagram, the cloud connector's IP address, 10.10.10.55, would be NAT'd to 203.0.113.2. For the Allowed Network, you would create a host network object with the value 203.0.113.2.

Step 4 Create an Access Control policy in Secure Firewall device manager that allows management traffic (HTTPS) from the public IP address of the SDC or cloud connector, to the outside interface of your FDM-managed device. In this scenario, the source address would be 203.0.113.2 and the source protocol would be HTTPS; the destination address would be 209.165.202.129 and the protocol would be HTTPS.

Step 5 **Deploy the change**. You can now manage the device using the outside interface.

What to do next

What if you are using a cloud connector?

The process is very similar, except for two things:

- In step 3c of the procedure above, your "Allowed Network" is a network group object containing the public IP addresses of the cloud connector. See Connecting Devices to Security Cloud Control Through the Cloud Connector for a list of Cloud Connector IP addresses for the various Security Cloud Control regions.
- In step 4 of the procedure above, you create an Access Control rule that allows access to the outside interface from the public IP addresses of the cloud connector.

The Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key approach is the recommended way of onboarding the FDM-managed device to Security Cloud Control. After you configure the outside interface to allow management access from the cloud connector, onboard the FDM-managed device. You will connect using the IP address of the outside interface. In our scenario, that address is 209.165.202.129.

Onboard an FDM-Managed Device to Security Cloud Control

Use the following procedures to onboard an FDM-managed to Security Cloud Control with the following methods.

Onboard an FDM-Managed Device Using Username, Password, and IP Address

Use this procedure to onboard an FDM-managed device using only the device credentials and the device's Management IP address. This is the simplest method of onboarding an FDM-managed device. However, the recommended way of onboarding an FDM-managed device to Security Cloud Control is by using a Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key.

Before you begin

Important Before you onboard an FDM-managed device to Security Cloud Control, read Onboard a Threat Defense Device and Connect Security Cloud Control to your Managed Devices, on page 15. They provide the general device requirements and onboarding prerequisites needed to onboard a device.

- You need the following information to onboard an FDM-managed device using the credentials method:
  - The device credentials Security Cloud Control will use to connect to the device.
  - The device's IP address of the interface you are using to manage the device. This may be the Management interface, an inside interface, or the outside interface depending on how you have configured your network.
  - The device must be managed by Secure Firewall device manager and configured for local management in order for you to onboard it to Security Cloud Control. It cannot be managed by Secure Firewall Management Center.

Note If you connect to https://eu.manage.security.cisco.com and your FDM-managed device is running software version 6.4, you must use this method. You can only onboard an FDM-managed device running software version 6.5+.

Procedure

Step 1 Log in to Security Cloud Control.

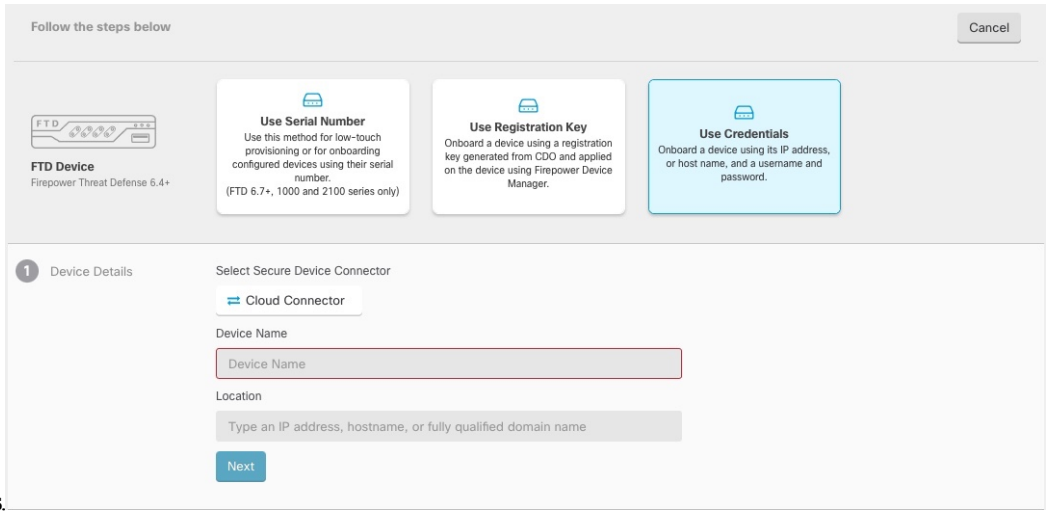
Step 2 In the left pane, click **Security Devices**.

Step 3 Click the blue plus button to **Onboard** a device.

Step 4 Click **FTD**.

Important When you attempt to onboard an FDM-managed device, Security Cloud Control prompts you to read and accept the Secure Firewall Threat Defense End User License Agreement (EULA), which is a one-time activity for your tenant. Once you accept the EULA, Security Cloud Control won't prompt you again to accept it unless the EULA changes.

Step 5 In the onboarding wizard, click **Use Credentials**.



Step 6 In the Device Details step:

- Click the **Secure Device Connector** button and select a Secure Device Connector (SDC) installed in your network. If you would rather not use an SDC, Security Cloud Control can connect to your FDM-managed device using the Cloud Connector. Your choice depends on how you Connect Security Cloud Control to your Managed Devices.
- Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- In the**Location** field, enter the IP address of the interface you are using to manage the device, hostname, or fully qualified domain name of the device. The default port is 443.

Important If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your Security Cloud Control tenant and SecureX/CTR account in order for your devices to be registered with SecureX. Your accounts can be merged through the SecureX portal. See Merge Your Security Cloud Control and SecureX Accounts for instructions. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

Step 7 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default. This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See Update FDM-Managed Device Security Databases and Schedule a Security Database Update.

Disabling this option does not affect any previously scheduled updates you may have configured through FDM.

Click **Next**.

Step 8 Enter the device administrator's username and password and click **Next**.

Step 9 If there are pending changes on the device's Secure Firewall device manager, you will be notified and you can revert the changes or log in to the manager and deploy the pending changes. If there are no pending changes on Secure Firewall device manager, you will not see a prompt.

Step 10 (Optional) Add a label the device. See Security Cloud Control Labels and Filtering for more information.

Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key

This procedure describes how to onboard an FDM-managed device using a registration key. This method is the recommended way of onboarding the FDM-managed device to Security Cloud Control and is beneficial if your FDM-managed device is assigned an IP address using DHCP. If that IP address changes for some reason, your FDM-managed device remains connected to Security Cloud Control. Additionally, your FDM-managed device can have an address on your local area network, and as long as it can access the outside network, it can be onboarded to Security Cloud Control using this method.

Warning If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your Security Cloud Control tenant and SecureX/CTR account in order for your devices to be registered with SecureX. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features. We **strongly** recommend merging your accounts before you create a Security Cloud Control module in SecureX. Your accounts can be merged through the SecureX portal. See Merge Accounts for instructions.

Before Onboarding

- For customers running version 6.4, this method of onboarding is only supported for the US region, https://us.manage.security.cisco.com.
- For customers running version 6.4, and connecting to the EU region, they must onboard their device using its Onboard an FDM-Managed Device Using Username, Password, and IP Address.
- Customers running version 6.5 or later, and connecting either to the US, EU, or APJ regions can use this method of onboarding.

- Review Connect Security Cloud Control to your Managed Devices, on page 15 for the networking requirements needed to connect Security Cloud Control to yourFDM-managed device.
- Make sure your device is managed by Secure Firewall device manager, not Secure Firewall Management Center.
- Devices running version 6.4 and 6.5 must not be registered with Cisco Smart Software Manager before onboarding them with a registration key. You will need to unregister the smart licenses of those FDM-managed devices before onboarding them to Security Cloud Control. See "Unregistering a Smart-licensed Firewall device manager" below.
- The device may be using a 90-day evaluation license.
- Log in to the FDM-managed device and make sure that there are no pending changes waiting on the device.
- Make sure DNS is configured properly on your FDM-managed device.
- Make sure the time services are configured properly on the FDM-managed device.
- Make sure the FDM-managed device shows the correct date and time otherwise the onboarding will fail.

What to do next

Do one of these two these things:

- Unregsiter your FDM-managed device from Cisco Smart Software Manager if it is already smart-licensed. **You must unregister the device from Cisco Smart Software Manager before you onboard it to Security Cloud Control with a registration Key.**Continue to Unregister a Smart-licensed FDM-Managed Device, on page 169.
- If your device is not already smart-licensed, continue to Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 170.

Unregister a Smart-licensed FDM-Managed Device

If the device you want to onboard is running version 6.4 or 6.5, and is already smart-licensed, the device is likely to be registered with Cisco Smart Software Manager. **You must unregister the device from Cisco Smart Software Manager before you onboard it to Security Cloud Control with a registration Key.** When you unregister, the base license and all optional licenses associated with the device, are freed in your virtual account.

After unregistering the device, the current configuration and policies on the device continue to work as-is, but you cannot make or deploy any changes.

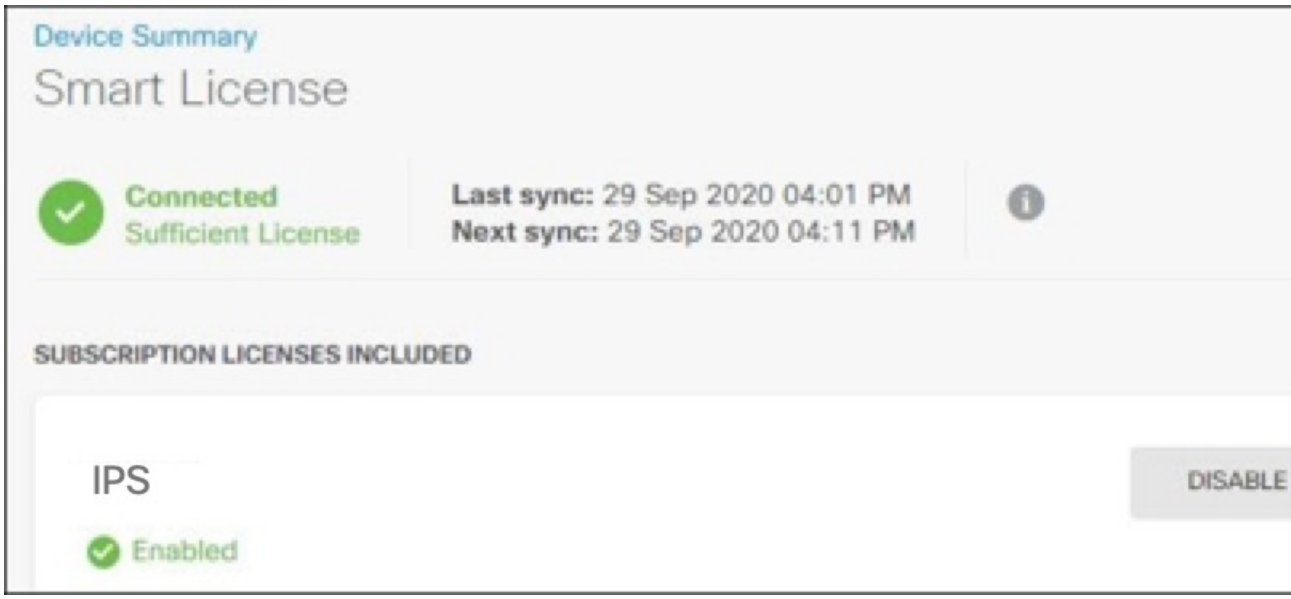
Procedure

Step 1 Log on to the device using the Secure Firewall device manager.

Step 2 Click the device icon in the upper tab.

Step 3 In the **Smart License** area, click **View Configuration**.

Step 4 Click the **Go to Cloud Services** gear menu and select **Unregister Device**.



Step 5 Read the warning and click **Unregister** to unregister the device.

What to do next

If you unregistered your in order to onboard it to Security Cloud Control, continue to Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 170

Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key

To onboard an FDM-managed using a registration key, follow this procedure:

Before you begin

Review the prerequisites discussed in Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 168.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Security Devices**.

Step 3 click the blue plus button  to **Onboard** a device.

Step 4 Click **FTD**.

Important When you attempt to onboard an FDM-managed device, Security Cloud Control prompts you to read and accept the Firepower Threat Defense End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, Security Cloud Control doesn't prompt it again in subsequent FDM-managed onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

Step 5 On the **Onboard FTD Device** screen, click **Use Registration Key**.

Step 6 Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.

Step 7 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** option is enabled by default. This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See Update FDM-Managed Device Security Databases and Schedule a Security Database Update for more information.

Note Disabling this option does not affect any previously scheduled updates you may have configured through Secure Firewall device manager.

Step 8 In the **Create Registration Key** area, Security Cloud Control generates a registration key.

Note If you move away from the onboarding screen after the key is generated and before the device is fully onboarded, you will not be able to return to the onboarding screen; however, Security Cloud Control creates a placeholder for that device on the **Inventory** page. When you select the device's placeholder, you will be able to see the key for that device in an action pane located to the right.

Step 9 Click the Copy icon to copy the registration key.

Note You can skip copying the registration key and click **Next** to complete the place holder entry for the device and later, register the device. This option is useful when you're attempting to create the device first and later register it or if you're a Cisco partner installing a Proof of Value (POV) device in a customer network.

On the **Inventory** page, you will see that the device is now in the connectivity state, "Unprovisioned". Copy the registration key appearing under **Unprovisioned** to Firewall device manager to complete the onboarding process.

Step 10 Log into the Secure Firewall device manager of the device you want to onboard to Security Cloud Control.

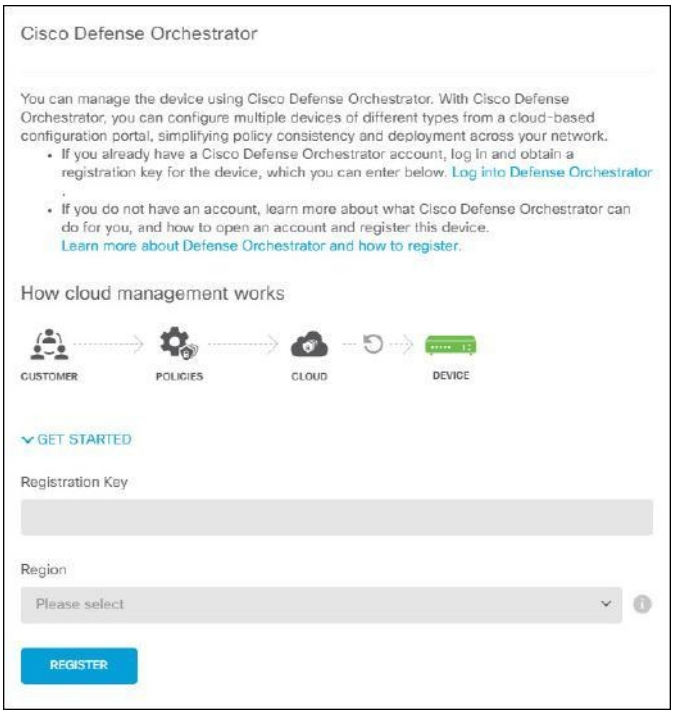
Step 11 In **System Settings**, click **Cloud Services**.

Step 12 In the Security Cloud Control tile, click **Get Started**.

Step 13 In the **Region** field, select the Cisco cloud region that your tenant is assigned to.

Note This step is not applicable FDM-managed devices running version 6.4.

Step 14 In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.



Step 15 Click **Register** and then **Accept** the Cisco Disclosure.

Step 16 Return to Security Cloud Control. Select all the licenses you want to apply to the device.

For more information, see Applying or Updating a Smart License. You can also click **Skip** to continue the onboarding with a 90-day evaluation license.

Step 17 Return to Security Cloud Control, open the **Inventory** page and see that the device status progresses from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key

This procedure describes how to onboard an FDM-managed device running Version 6.6+ using a registration key. This method is the recommended way of onboarding the FDM-managed device to Security Cloud Control and is beneficial if your FDM-managed device is assigned an IP address using DHCP. If that IP address changes for some reason, your FDM-managed device remains connected to Security Cloud Control. Additionally, your FDM-managed device can have an address on your local area network, and as long as it can access the outside network, it can be onboarded to Security Cloud Control using this method.

Warning If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your Security Cloud Control tenant and SecureX/CTR account in order for your devices to be registered with SecureX. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features. We **strongly** recommend merging your accounts before you create a Security Cloud Control module in SecureX. Your accounts can be merged through the SecureX portal. See Merge Accounts for instructions.

If you want to onboard an FDM-managed device running version 6.4 or 6.5, see Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key.

Before Onboarding

- This method of onboarding is currently available for version 6.6+ and to customers connecting to https://us.manage.security.cisco.com, https://eu.manage.security.cisco.com, or https://apj.manage.security.cisco.com.
- **Review** Connect Security Cloud Control to your Managed Devices, on page 15 for the networking requirements needed to connect Security Cloud Control to your FDM-managed device.
- Make sure your device is managed by Secure Firewall device manager, not Secure Firewall Management Center.
- The device can be using a 90-day evaluation license or it can be smart-licensed. Devices running version 6.6+ can be onboarded to Security Cloud Control using a registration key without unregistering any installed smart licenses.
- The device cannot already be registered with Cisco Cloud Services. See "Unregistering an FDM-Managed Device from Cisco Cloud Services" below before onboarding.
- Log in to the device's Secure Firewall device manager UI and make sure that there are no pending changes waiting on the device.
- Make sure DNS is configured properly on your FDM-managed device.
- Make sure the time services are configured on the FDM-managed device.
- Make sure the FDM-managed device shows the correct date and time otherwise the onboarding will fail.

What to do next:

Do one of these things:

- If your FDM-managed device running verison 6.6+ is already registered with Cisco Cloud Services, you need to unregister the device before onboarding it. Continue to Unregistering an FDM-Managed Device from Cisco Cloud Services, on page 173.
- If your device is not registered to Cisco Cloud Services, continue to Procedure to Onboad an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, on page 174.

Unregistering an FDM-Managed Device from Cisco Cloud Services

The following procedure is how to unregister the device from Cisco Cloud Services. Use this method before you onboard and FDM-managed device to Security Cloud Control with a registration key.

Note If you onboard a virtual FDM-managed device running version 7.0 or later, registering the virtual FDM-managed device to Security Cloud Control automatically resets the performance-tiered Smart Licensing selection to **Variable**, which is the default tier. You **must** manually re-select the tier that matches the license associated with the device through the Secure Firewall device manager UI after onboarding.

Use this procedure to check and make sure it is not registered to Cisco Cloud Services:

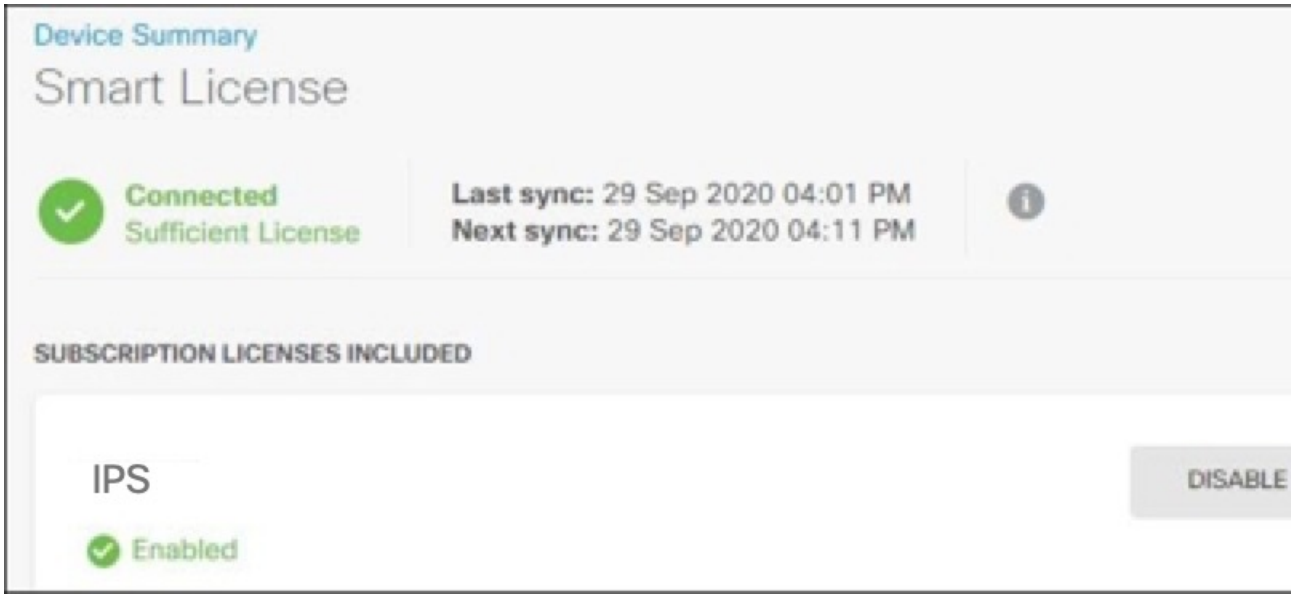
Procedure

Step 1 Log on to the device using Secure Firewall device manager.

Step 2 Click the device icon in the upper tab.

Step 3 Expand the **System Settings** menu and then click **Cloud Services**.

Step 4 In the **Cloud Services** page, click the gear menu and select **Unregister Cloud Services**.



Step 5 Read the warning and click **Unregister** to unregister the device.

What to do next

If you are trying to onboard a FDM-managed device running version 6.6 or later, continue to Procedure to Onboad an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, on page 174.

Procedure to Onboad an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key

To onboard an FDM-managed device using a registration key, follow this procedure:

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the blue plus button to **Onboard** a device.

Step 4 Click **FTD**.

Important When you attempt to onboard the FDM-managed device, Security Cloud Control prompts you to read and accept the End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, Security Cloud Control doesn't prompt it again in subsequent onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

Step 5 On the **Onboard FTD Device** screen, click **Use Registration Key**.

Step 6 Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.

Step 7 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default. This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See Update FDM-Managed Device Security Databases and Schedule a Security Database Update for more information.

Note Disabling this option does not affect any previously scheduled updates you may have configured through Secure Firewall device manager.

Step 8 In the **Create Registration Key** step, Security Cloud Control generates a registration key.

Note If you move away from the onboarding screen after the key is generated and before the device is fully onboarded, you will not be able to return to the onboarding screen; however, Security Cloud Control creates a placeholder for that device on the **Inventory** page. When you select the device's placeholder, you will be able to see the key for that device, on that page.

Step 9 Click the Copy icon to copy the registration key.

Note You can skip copying the registration key and click **Next** to complete the place holder entry for the device and later, register the device. This option is useful when you're attempting to create the device first and register it later, or if you're a Cisco partner installing a Proof of Value (POV) device in a customer network.

On the **Inventory** page, you will see that the device is now in the connectivity state, "Unprovisioned". Copy the registration key appearing under **Unprovisioned**to Firewall device manager to complete the onboarding process.

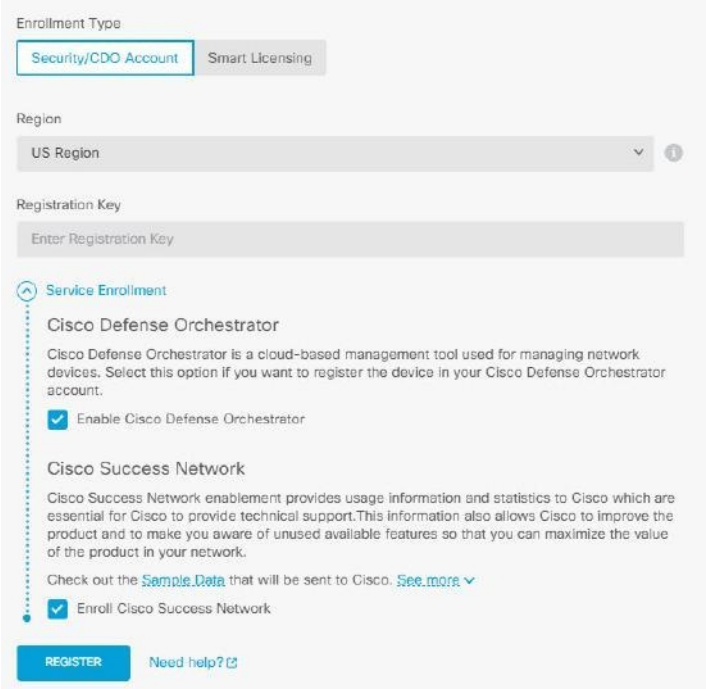
Step 10 Log into the Secure Firewall device manager of the device you are onboarding.

Step 11 Under **System Settings**, click **Cloud Services**.

Step 12 In the **Region** field, select the Cisco cloud region that your tenant is assigned to.

Step 13 In the **Enrollment Type** area, click **Security Account** .

Note For devices running version 6.6, note that the Tenancy tab for Security Cloud Control is titled **Security Account** and you must manually enable Security Cloud Control in Secure Firewall device manager.



Step 14 In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.

Step 15 For devices running version 6.7 or later in the Service Enrollment area, check **Enable Cisco Security Cloud Control**.

Step 16 Review the information about the Cisco Success Network Enrollment. If you do not want to participate, uncheck the **Enroll Cisco Success Network** checkbox.

Step 17 Click **Register** and then **Accept** the Cisco Disclosure. Secure Firewall device manager sends the registration request to Security Cloud Control.

Step 18 Return to Security Cloud Control, in the **Create Registration Key** area, click **Next**.

Step 19 Select all licenses you want to apply to the device. Click **Next**.

Step 20 Return to Security Cloud Control, open the **Inventory** page and see that the device status progresses from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed Device using the Device's Serial Number

This procedure is a simplified method of setting up and onboarding the FDM-managed devices to Security Cloud Control. All you need is the chassis serial number or PCA serial number of the device. You can apply a smart license or use a 90-day evaluation license when onboarding the device.

Ensure that you read through the use cases to understand the concepts before you perform the Workflow and Prerequisites to Onboard the FDM-Managed Device Using Zero-Touch Provisioning.

Important These methods of onboarding FDM-managed devices are only available for devices running version 6.7 or higher.

Use Cases

- Onboard an FDM-Managed Device using the Device's Serial Number, on page 176: Onboarding a new factory-shipped FDM-managed device that is added to a network and reached from the Internet. The initial device setup wizard is not complete on the device.
- Onboard a Configured FDM-Managed Device using the Device's Serial Number, on page 184: Onboarding an already configured FDM-managed device or an upgraded device that is already added to a network and reached from the Internet. The initial device setup wizard is complete on the device.

Important If you want to use this method to onboard a device running on an older software version that is supported for your device, you need to perform a fresh installation (reimage) of the software on that device instead of an upgrade.

Related Information:

- Terminologies and Definitions used in Zero-Touch Provisioning
- Troubleshoot FDM-Managed Device Onboarding Using Serial Number

Workflow and Prerequisites to Onboard the FDM-Managed Device Using Zero-Touch Provisioning

Zero-Touch Provisioning is a feature that allows a new factory-shipped Firepower 1000, Firepower 2100, or Secure Firewall 3100 series device to be provisioned and configured automatically, eliminating most of the manual tasks involved with onboarding the device to Security Cloud Control. The zero-touch provisioning is intended for remote offices or other locations where your employees are less experienced working with networking devices.

To use the zero-touch provisioning process, you must onboard the device to Security Cloud Control, connect it to a network that can reach the internet, and power on the device. See Onboard a Configured FDM-Managed Device using the Device's Serial Number, on page 184 for more information.

Note You can power-on the device before or after onboarding it to Security Cloud Control. **We recommend that you onboard the device to Security Cloud Control first and power-on the device and connect it to your branch network second.** When you onboard the device in Security Cloud Control, the device is associated with your Security Cloud Control tenant in the Cisco cloud and Security Cloud Control automatically syncs the device configuration.

You can also use this procedure to onboard a device purchased from an external vendor or onboard a device already managed by another cloud tenant in a different region. However, if the device is already registered to the external vendor's cloud tenant or a cloud tenant in a different region, Security Cloud Control doesn't onboard the device but displays the "*Device serial number already claimed*" error message. In such cases, the Security Cloud Control admin must unregister the device's serial number from its previous cloud tenant and then claim the Security Cloud Control device in their own tenant. See Device Serial Number Already Claimed in the troubleshooting chapter.

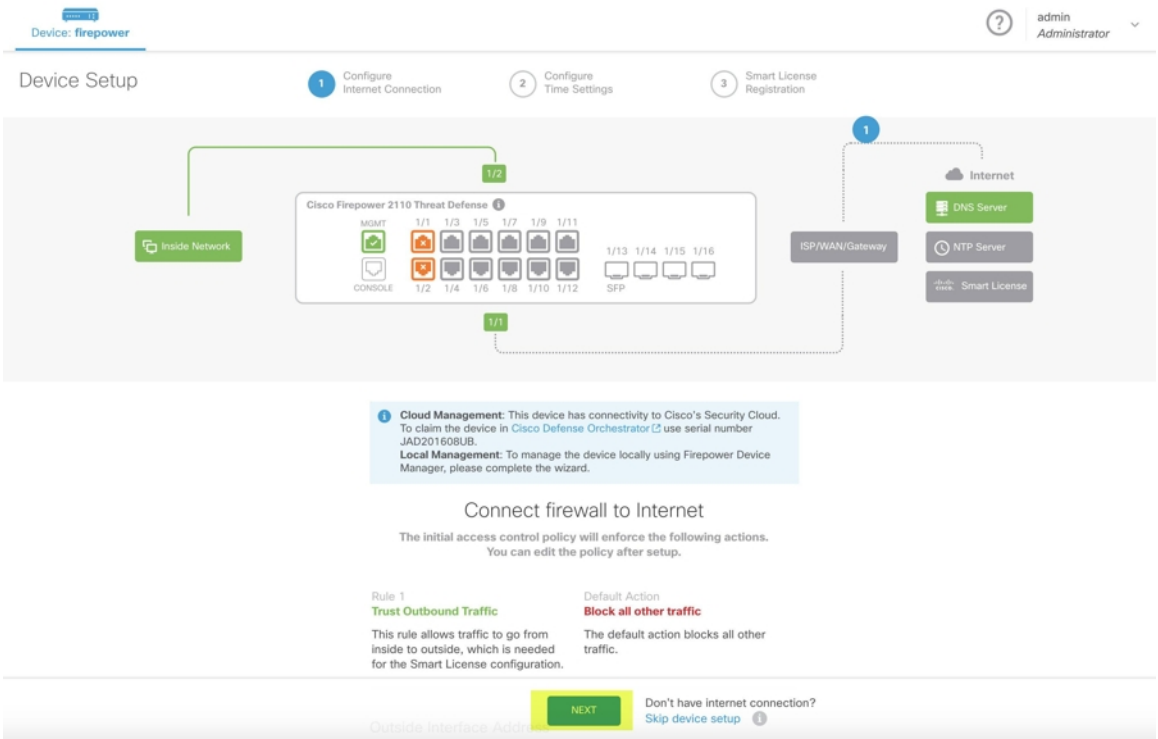
The device **Connectivity** status changes to "Online" and the **Configuration** status changes to "Synced". The FDM-managed device is onboarded to Security Cloud Control.

You can see the Status LED (Firepower 1010), SYS LED (Firepower 2100), or S LED Secure Firewall 3100) flashing green on the rear panel of the hardware. The device LED continues to flash in green when it's connected to the cloud. If the device can't connect to the Cisco cloud or loses its connectivity after being connected, you can see the Status LED (Firepower 1010), SYS LED (Firepower 2100), or M LED (Secure Firewall 3100) flashing alternate green and amber.

See this video: Installing Your Cisco Firepower Firewall Using Zero-Touch Provisioning video to understand the LED indicators.

Important If you have logged into the FDM-managed device console, SSH, or Secure Firewall Threat Defense, you would have changed the device's password during your first login. You can still use the zero-touch provisioning process for onboarding the device using Security Cloud Control. After you log into Secure Firewall Threat Defense, ensure that you do not complete the device setup wizard step that configures the outside interface. If you complete this step, the device is unregistered from the cloud, and you cannot use the zero-touch provisioning process.

When you log into Secure Firewall Threat Defense, you will see the following screen on the dashboard.



Without proceeding further on the Secure Firewall Threat Defense UI, go to the serial number onboarding wizard and onboard the device. Here, you must select **Default Password Changed** because the device password has already been changed.

Prerequisites

Software and Hardware Requirements

The FDM-managed devices must be running software that supports serial-number-onboarding. Use the following table as a guide:

Table 7: Hardward and Software Support

Firewall Model Numbers that Support Zero-Touch Provisioning	Supported Firewall Software Version	Software Package
Firepower 1000 series device models: 1010, 1120, 1140, 1150	6.7 or later	SF-F1K-TDx.x-K9
Firepower 2100 series device models: 2110, 2120, 2130, 2140	6.7 or later	SF-F2K-TDx.x-K9
Secure Firewall 3100 series device models: 3110, 3120, 3130, 3140	7.1 or later	SF-F3K-TDx.x-K9

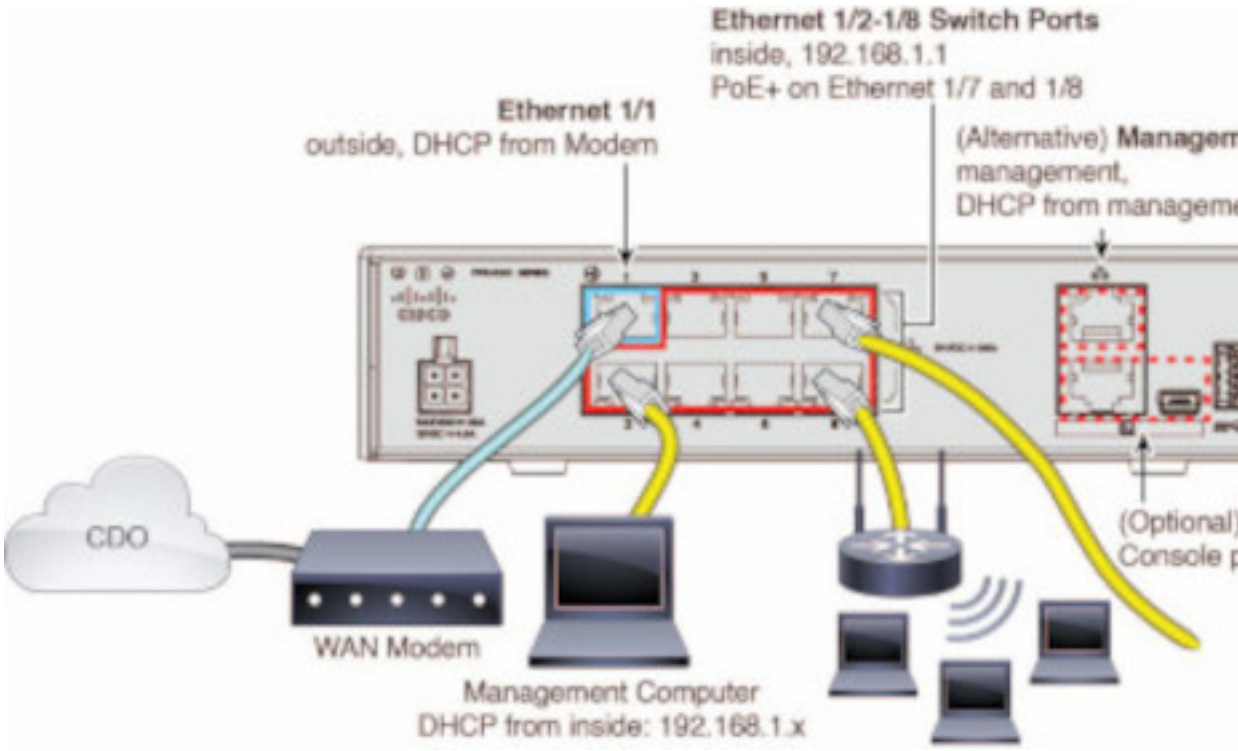
Confirm the management platforms are running the correct version.

Table 8: Support FTD Manager Versions

Manager	Supported Version
Secure Firewall Device Manager	7.0 or later
On-Premises Firewall Management Center	7.2 or later
Cloud-delivered Firewall Management Center	Not applicable

Configuration Prerequisites for Hardware Installation

- **The network at the branch office cannot use the 192.168.1.0/24 address space.** The network on Ethernet 1/1 (outside) cannot use the 192.168.1.0/24 address space. The default IP address of the Ethernet 1/2 "inside" interface on the 1000 and 2100 series devices running FDM 6.7 is 192.168.1.1 may conflict with the DHCP address allocated by your WAN modem if it's on that subnet.
  - **inside** - Ethernet 1/2, IP address 192.168.1.1
  - **outside** - Ethernet 1/1, IP address from DHCP or an address you specify during setup



If you are unable to change the outside interface settings, use Secure Firewall device manager to change the subnet on the Ethernet 1/2 "inside" interface settings to avoid conflict. For example, you could change to the following subnet settings:

- IP Address: 192.168.95.1
- DHCP server range: 192.168.95.5-192.168.95.254

To learn about the steps for configuring the physical interface, see the "Secure Firewall Device Manager Configuration Guide". In the "Interfaces" chapter, see the "Configure a Physical Interface" section.

- The threat defense device must be installed and connected to the Cisco Cloud.
- The outside or management interface of the device must be connected to a network providing DHCP addressing. Typically, the device has a default DHCP client on the outside or management interface.

Note If the management interface is connected to a network having a DHCP server, it takes precedence over the outside interface for Linux stack initiated traffic.

- Your outside or management interface needs to access to be able to access the following Security Services Exchange domains for the serial onboarding method.
  - Australia Region
    - api.aus.sse.itd.cisco.com
    - est.sco.cisco.com (common across geographies)
    - mx*.aus.sse.itd.cisco.com (currently only mx01.aus.sse.itd.cisco.com)

  - dex.aus.sse.itd.cisco.com (for customer success)
  - eventing-ingest.aus.sse.itd.cisco.com (for CTR and Security Cloud Control)
  - registration.aus.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)

- APJ Region
  - api.apj.sse.itd.cisco.com
  - est.sco.cisco.com (common across geographies)
  - mx*.apj.sse.itd.cisco.com (currently only mx01.apj.sse.itd.cisco.com)
  - dex.apj.sse.itd.cisco.com (for customer success)
  - eventing-ingest.apj.sse.itd.cisco.com (for CTR and Security Cloud Control)
  - http://registration.apj.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)

- EU Region
  - api.eu.sse.itd.cisco.com
  - est.sco.cisco.com (common across geographies)
  - mx*.eu.sse.itd.cisco.com (currently only mx01.eu.sse.itd.cisco.com)
  - dex.eu.sse.itd.cisco.com (for customer success)
  - eventing-ingest.eu.sse.itd.cisco.com (for CTR and Security Cloud Control)
  - registration.eu.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)

- India Region
  - api.in.sse.itd.cisco.com
  - est.sco.cisco.com (common across geographies)
  - mx*.in.sse.itd.cisco.com (currently only mx01.in.sse.itd.cisco.com)
  - dex.in.sse.itd.cisco.com (for customer success)
  - eventing-ingest.in.sse.itd.cisco.com (for CTR and Security Cloud Control)
  - registration.in.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)

- US Region
  - api-sse.cisco.com
  - est.sco.cisco.com (common across geographies)
  - mx*.sse.itd.cisco.com (currently only mx01.sse.itd.cisco.com)
  - dex.sse.itd.cisco.com (for customer success)
  - eventing-ingest.sse.itd.cisco.com (for CTR and Security Cloud Control)

- registration.us.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)

- The outside interface of the device must have DNS access to Cisco Umbrella DNS.

Before Claiming the Device in Security Cloud Control

Before claiming the device in Security Cloud Control, make sure that you have the following information:

- Chassis serial number or PCA number of the threat defense device. You can find this information on the bottom of the hardware chassis or on the carton box in which your device is delivered. In the following example picture, you can see the serial number "*******X0R9" on the bottom of the Firepower 1010 chassis.

- The default password of the device.

- A smart license generated from Cisco Smart Software Manager for using the additional capabilities. However, you can complete the device onboarding using a 90-day evaluation license and later apply the smart license.

Onboard a Secure Firewall Threat Defense Device With Zero-Touch Provisioning

Caution When the device is being onboarded in Security Cloud Control, we recommend that you not perform the device easy setup using the Secure Firewall device manager. This causes provisional error in Security Cloud Control.

Before you begin

- The threat defense device must not be prevously or currently managed by Firewall Device Manager or Management Center. If the device is currently managed by a platform, see Onboard a Configured FDM-Managed Device using the Device's Serial Number, on page 184.
- If you onboard a device with the intention of managing it with an on-premises management center, the on-premises management center **must** be running version 7.4 and later.

Procedure

Step 1 If you are onboarding a device purchased from an external vendor, you must reimage the device first. For more information, see the "Reimage Procedures" chapter of the Cisco FXOS Troubleshooting Guide.

Step 2 Log in to Security Cloud Control.

Step 3 In the navigation pane, click **Security Devices**.

Step 4 Click the blue plus button  to **Onboard** a device.

Step 5 Click the **FTD** tile.

Important When you attempt to onboard a device, Security Cloud Control prompts you to read and accept the End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, Security Cloud Control doesn't prompt it again in subsequent onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

Step 6 On the **Onboard FTD Device** screen, click **Use Serial Number**.

Step 7 In the **Select FMC** step, use the drop-down menu to select an on-premises management center that has already been onboarded to Security Cloud Control. Click **Next**.

The on-premises management center must be running version 7.4 or higher. If you do not have an on-premises management center onboarded, click +Onboard On-Prem FMC for the onboarding wizard.

Step 8 In the **Connection** step, enter the device's serial number and device name. Click **Next**.

Step 9 For zero-touch provisioning, the device must be brand new, or has been reimaged. For the **Password Reset**, be sure to select **Yes, this new device has never been logged into or configured for a manager**. Enter a new password and confirm the new password for the device, then click **Next**.

Step 10 For **Policy Assignment**, use the drop-down menu to select a access control policy to be deployed once the device is onboarded. If you do not have a customized policy, Security Cloud Control auto-selects the default access control policy. Click **Next**.

Step 11 Select all licenses you want to apply to the device. Click **Next**.

Step 12 (Optional) Add labels to the device. Security Cloud Control applies these labels once the device successfully onboards.

What to do next

Security Cloud Control starts claiming the device, and you will see the **Claiming** message on the right. Security Cloud Control continuously polls for an hour to determine if the device is online and registered to the cloud.

Once it's registered to the cloud, Security Cloud Control starts the initial provisioning and onboards the device successfully. The device registration can be confirmed when the LED status flashes green on the device. If the device can't connect to the Cisco cloud or lose its connectivity after being connected, you can see the Status LED (Firepower 1000) or SYS LED (Firepower 2100) flashing alternate green and amber.

If the device is still not registered to the cloud within the first one hour, a time-out occurs, and now Security Cloud Control polls periodically for every 10 minutes to determine the device status and remain in **Claiming** state. When the device is turned on and connected to the cloud, you don't have to wait for 10 minutes to know its onboarding status. You can click the **Check Status** link anytime to see the status. Security Cloud Control starts the initial provisioning and onboards the device successfully.

Important Suppose you have already completed the device setup wizard (see Onboard a Configured FDM-Managed Device using the Device's Serial Number), the device is unregistered from the cloud, and in this case, Security Cloud Control remains in **Claiming** state. You need to complete manual registration from Secure Firewall device manager to add it to Security Cloud Control. (In Secure Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Security Cloud Control** option and click **Register**). Then, click **Check Status**.

Onboard a Configured FDM-Managed Device using the Device's Serial Number

This procedure is for devices that have already been configured for local management. Because the device setup wizard is completed on an already configured FDM-managed device, the device is unregistered from the cloud, and you can't onboard such devices to Security Cloud Control using the zero-touch provisioning process.

If you device is brand new and has never been managed or configured, you can onboard the device with zero-touch provisioning. See Onboard a Secure Firewall Threat Defense Device With Zero-Touch Provisioning, on page 182 for more information.

Note When the device is not connected to the Cisco cloud, you can see the Status LED (Firepower 1000), SYS LED (Firepower 2100), or M LED (Secure Firewall 3100) flashing alternate green and amber.

You may have completed the device setup wizard to perform the following tasks:

- The device must be running version 6.7 or later.
- Configure a static IP address on the management interface of the device. If the interfaces cannot obtain the necessary dynamic IP address, or the DHCP server does not provide the gateway route, you need to configure a static IP address.
- Obtain an address using PPPoE and configure the outside interface.
- Manage the device running version 6.7 or later device using Secure Firewall device manager or Secure Firewall Management Center.
- You have an active SecureX account. If you do not have a SecureX account, see SecureX and Security Cloud Control for more information.
- Your Security Cloud Control and SecureX account are merged. See Link Your Security Cloud Control and SecureX or Cisco XDR Tenant Accounts for more information.

Important You can switch the manager of a Secure Firewall Threat Defense device from Secure Firewall device manager to Secure Firewall Management Center, or the other way. Perform the steps explained in the **Switching Between Local and Remote Management** section of the "System Management" chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version the device runs.

If you want to onboard devices, perform the following:

Procedure

Step 1 Review the prerequisites for onboarding here Workflow and Prerequisites to Onboard the FDM-Managed Device Using Zero-Touch Provisioning.

Step 2 In the Secure Firewall device manager UI, navigate to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Security Cloud Control** option and click **Register**.

Step 3 Log in to Security Cloud Control.

Step 4 In the navigation pane, click **Security Devices**.

Step 5 Click the **FTD tile.**

Step 6 On the **Onboard FTD Device** screen, click **Use Serial Number**.

Step 7 In the **Select FMC** step, use the drop-down menu to select an on-premises management center that has already been onboarded to Security Cloud Control. Click **Next**.

The on-premises management center must be running version 7.4 or higher. If you do not have an on-premises management center onboarded, click +Onboard On-Prem FMC for the onboarding wizard.

Step 8 In the **Connection** step, enter the device's serial number and device name. Click **Next**.

Step 9 If the device is **not** brand new and has already been configured for management, select **Yes, this new device has never been logged into or configured for a manager** for the **Password Reset**. Click **Next**.

Step 10 For **Policy Assignment**, use the drop-down menu to select a access control policy to be deployed once the device is onboarded. If you do not have a customized policy, Security Cloud Control auto-selects the default access control policy. Click **Next**.

Step 11 Select all licenses you want to apply to the device. Click **Next**.

Security Cloud Control changes the device **Connectivity** status changes to "Online" and the **Configuration** status changes to the "Synced" state. The FDM-managed device is onboarded to Security Cloud Control. You can see the Status LED (Firepower 1000), SYS LED (Firepower 2100), or M LED flashing green on the rear panel of the hardware. The device LED continues to flash in green when it's connected to Cisco Cloud. If the device can't connect to the Cisco cloud or loses its connectivity after being connected, you can see the same status LED flash alternate green and amber.

Related Information:

- Terminologies and Definitions used in Zero-Touch Provisioning

Onboard an FDM-Managed High Availability Pair

To onboard an Secure Firewall Threat Defense HA pair to Security Cloud Control, you must onboard each device of the pair individually. Once both peers of the pair are onboarded Security Cloud Control automatically combines them as a single entry in the **Inventory** page. Onboard the devices using either the device login credentials or a registration key. We recommend onboarding **both** devices with the same method. Also be aware that if you onboard a device that is in standby mode first, Security Cloud Control disables the ability to deploy or read from that device. You can only read or deploy to the active device within an HA pair.

Note Security Cloud Control strongly recommends onboarding devices with a registration key. Onboarding with a registration key is slightly different for Threat Defense devices running specific versions. See Onboard an FDM-Managed HA Pair Running Version 6.4 or Version 6.5, on page 186 and Onboard an FDM-Managed HA Pair Running Threat Defense Version 6.6 or Version 6.7 and later, on page 188 for more information.

Before you onboard an Threat Defense HA pair to Security Cloud Control, review the following:

- Your HA pair is already formed prior to onboarding to Security Cloud Control.
- Both devices are in a healthy state. The pair could be either primary/active and secondary/standby **or** primary/standby and secondary/active modes. Unhealthy devices will not successfully sync to Security Cloud Control.
- Your HA pair is managed by Secure Firewall device manager, not Secure Firewall Management Center.
- Your cloud connector connects to Security Cloud Control at https://us.manage.security.cisco.com.

Onboard an FDM-Managed High Availablity Pair with a Registration Key

Be aware of the following prerequisites before you onboard an FDM-managed High Availability (HA) pair with a registration key:

- Onboarding devices that are running version 6.4 with a registration key is only supported for the US region (https://us.manage.security.cisco.com). To connect to the EU region (https://eu.manage.security.cisco.com) they must onboard their HA pair with username, password, and IP address.
- Customers running version 6.5 or later, and connecting either to the US, EU, or APJ regions can use this method of onboarding.
- Devices running version 6.4 and 6.5 must not be registered with Cisco Smart Software Manager before onboarding them with a registration key. You will need to unregister the smart licenses of those FDM-managed devices before onboarding them to Security Cloud Control. See Unregister a Smart-licensed FDM-Managed Device, on page 169 for more information.

Onboard an FDM-Managed HA Pair Running Version 6.4 or Version 6.5

To onboard an FDM-managed HA pair running software version 6.4 or 6.5, you must onboard the devices one at a time. It does not matter if you onboard the active or standby, the primary or secondary device.

Note If you onboard either device of an HA pair with a registration key, you must onboard the other peer device in the same method.

Use the following steps for onboard an HA pair running Version 6.4 or 6.5:

Procedure

Step 1 Onboard a peer device. See Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 170 to onboard the first device within the pair.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the **FTD** tab. Once the device is synced, select the device so it is highlighted. In the action pane located directly below **Device Details**, click **Onboard Device**.

Step 5 Enter the **HA Peer Device Name** for the peer device that has already been onboarded. Click **Next**.

Step 6 If you provided a smart license for the first device, Security Cloud Control repopulates that license so you can use it for onboarding this current device. Click **Next**.

Note If you unregistered your device's Smart License to onboard your FDM-managed device, this is where you re-apply the smart license.

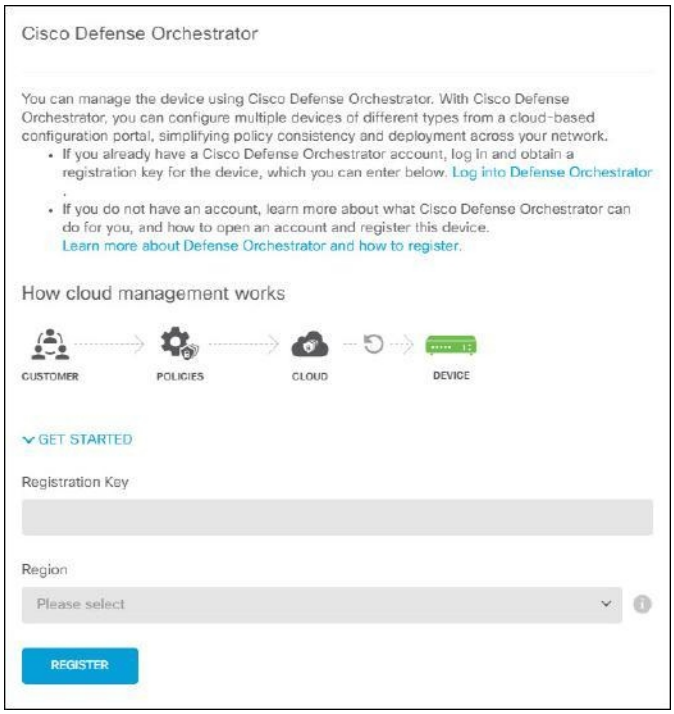
Step 7 Security Cloud Control automatically generates that registration key for the device you are preparing to onboarding. Click the **Copy** icon to copy the registration key.

Step 8 Log into the Secure Firewall device manager UI of the device you are onboarding.

Step 9 In **System Settings**, click **Cloud Services**.

Step 10 In the Security Cloud Control tile, click **Get Started**.

Step 11 In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.



Step 12 In the **Region** field, select the Cisco cloud region that your tenant is assigned to.

Note This step is not applicable to the FDM-managed device running on version 6.4.

Step 13 Click **Register** and then **Accept** the Cisco Disclosure.

Step 14 Return to Security Cloud Control and, in the **Create Registration Key** area, click **Next**.

Step 15 Click **Go to Inventory**. Security Cloud Control automatically onboards the device and combines them as a single entry. Similar to the first peer device you onboard, the device status changes from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed HA Pair Running Threat Defense Version 6.6 or Version 6.7 and later

To onboard an FDM-managed HA pair running threat defense version 6.6 or 6.7, you must onboard the device one at a time. It does not matter if you onboard the active or standby, the primary or secondary device.

Note If you onboard either device of an HA pair with a registration key, you must onboard the other peer device in the same method.

Use the following steps for onboard an HA pair running version 6.6 or 6.7:

Procedure

Step 1 Onboard a peer device. See Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, on page 172

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the **FTD** tab. Once the device is synced, select the device so it is highlighted. In the action pane located directly below **Device Details**, click **Onboard Device**.

Step 5 Enter the HA Peer Device Name for the peer device that has already been onboarded. Click **Next**.

Step 6 If you provided a smart license for the first device, Security Cloud Control repopulates that license so you can use it for onboarding this current device. Click **Next**.

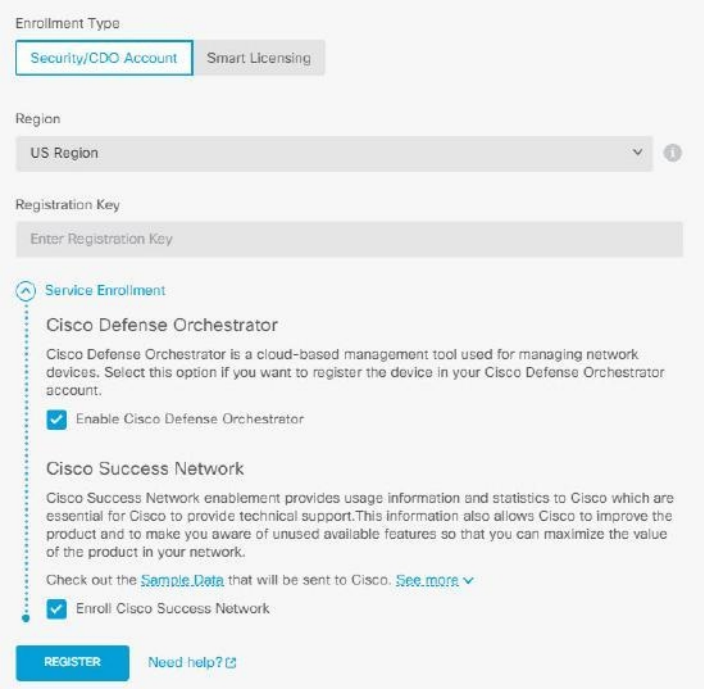
Step 7 Security Cloud Control automatically generates that registration key for the device you are preparing to onboarding. Click the Copy icon to copy the registration key.

Step 8 Log into the Secure Firewall device manager UI of the device you want to onboard to Security Cloud Control.

Step 9 Under **System Settings**, click **Cloud Services**.

Step 10 In the **Enrollment Type** area, click **Security/Security Cloud Control Account**.

Note For devices running version 6.6, note that the Tenancy tab for Security Cloud Control is titled **Security Account** and you must manually enable Security Cloud Control in the Secure Firewall device manager UI.



Step 11 In the **Region** field, select the Cisco cloud region that your tenant is assigned to.

Step 12 In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.

Step 13 For devices running version 6.7 or later in the Service Enrollment area, check **Enable Cisco Security Cloud Control**.

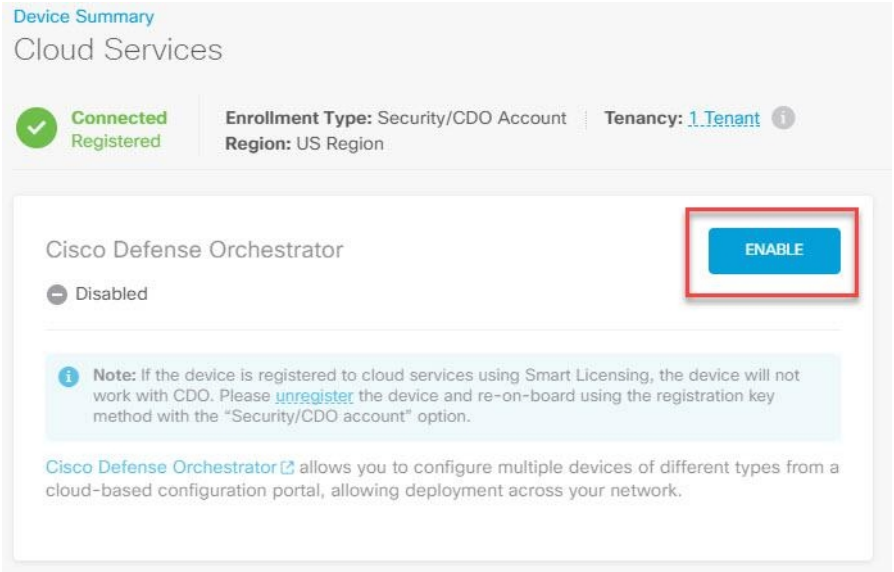
Step 14 Review the information about the Cisco Success Network Enrollment. If you do not want to participate, uncheck the **Enroll Cisco Success Network** check box.

Step 15 Click **Register** and then **Accept** the Cisco Disclosure. FDM sends the registration request to Security Cloud Control.

Step 16 Return to Security Cloud Control, in the **Create Registration Key** area, click **Next**.

Step 17 In the **Smart License** area, you can apply a smart license to the FDM-managed device and click **Next**or you can click **Skip** to continue the onboarding with a 90-day evaluation license or if the device is already smart-licensed. For more information, see Updating an Existing Smart License of an FDM-Managed Device, on page 195.

Note If your device is running version 6.6, you need to manually enable communication to Security Cloud Control. From the device's FDM-managed UI, navigate to **System Settings** > **Cloud Services** and, in the **Cisco Security Cloud Control** tile, click **Enable**.



Step 18 Return to Security Cloud Control, click **Go to Inventory**. Security Cloud Control automatically onboards the device and combines them as a single entry. Similar to the first peer device you onboard, the device status changes from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed High Availability Pair

Note Whichever method you onboard the first device of an HA pair with, you must onboard the other peer device in the same method.

To onboard an FDM-managed HA pair that has been created outside of Security Cloud Control, follow this procedure:

Procedure

Step 1 Onboard one of the peer devices within the HA pair. Onboard the device with its Onboard an FDM-Managed Device Using Username, Password, and IP Address, Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, or Onboard a Secure Firewall Threat Defense Device With Zero-Touch Provisioning.

Step 2 Once the device is synced, in the **Security Devices** page, click the **Devices** tab.

Step 3 Click the **FTD** tab.

Step 4 Select the device. In the action pane located directly below **Device Details**, click **Onboard Device**.

Step 5 In the pop-up window, enter the HA peer's device name and location.

Step 6 Click **Onboard Device**. Once both devices are successfully synced to Security Cloud Control, the HA pair is displayed as a single entity in the **Inventory** page.

Onboard an FTD Cluster

•

Onboard a Clustered Secure Firewall Threat Defense Device

Onboard a threat defense device that has already been clustered with the following procedure:

Before you begin

The following devices support clustering:

- Secure Firewall 3100 devices
- Firepower 4100 devices
- Firepower 9300 devices
- Threat Defense Virtual device (AWS, Azure, VMware, KVM, GCP)

Note the following limitations for clustered devices:

- Devices must be running at least version 6.4.
- Devices must be managed by a physical or virtual Secure Firewall Management Center.
- Firepower 4100 and Firepower 9300 devices must be clustered through the device's chassis manager.
- Secure Firewall 3100 devices, KVM, and VMware environments must be clustered through the Secure Firewall Management Center UI.
- Azure, AWS, and GCP environment clusters must be created through their own environment and onboarded to Secure Firewall Management Center.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the blue plus button  to **Onboard** a device.

Step 4 Click **FTD**.

Step 5 Under **Management Mode**, be sure **FTD** is selected.

By selecting **FTD**, you are retaining Secure Firewall Management Center as the managing platform. If you select **FDM**, this switches the manager from Secure Firewall Management Center to a local manager such as the Firewall Device Manager or cloud-delivered Firewall Management Center. Note that Switching managers resets all existing policy configurations except for interface configurations and you must re-configure policies after you onboard the device.

Step 6 On the **Onboard FTD Device** screen, click **Use CLI Registration Key**.

Step 7 Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.

Step 8 In the Policy Assignment step, use the drop-down menu to select an access control policy to deploy once the device is onboarded. If you have no policies configured, select the **Default Access Control Policy**.

Step 9 Specify whether the device you are onboarding is a physical or virtual device. If you are onboarding a virtual device, you must select the device's performance tier from the drop-down menu.

Step 10 Select the essentials licenses you want applied to the device. Click **Next**.

Step 11 Security Cloud Control generates a command with the registration key. Paste the entire registration key as is into the device's CLI.

Step 12 The device starts to onboard. As an optional step, you can add labels to your device to help sort and filter the Inventory page. Enter a label and select the blue plus button. .

What to do next

Once the device is sychronized, Security Cloud Control automatically detects that the device is clustered. From here, select the device you just onboarded from the Inventory page and select any of the options listed under the Management pane located to the right. We strongly recommend the following actions:

- If you did not already, create a custom access control policy to customize the security for your environment. See FDM-Managed Access Control Policy, on page 328 for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics.

Applying or Updating a Smart License

Applying a New Smart License to an FDM-Managed Device

Perform one of the following procedures to Smart License the FDM-managed device:

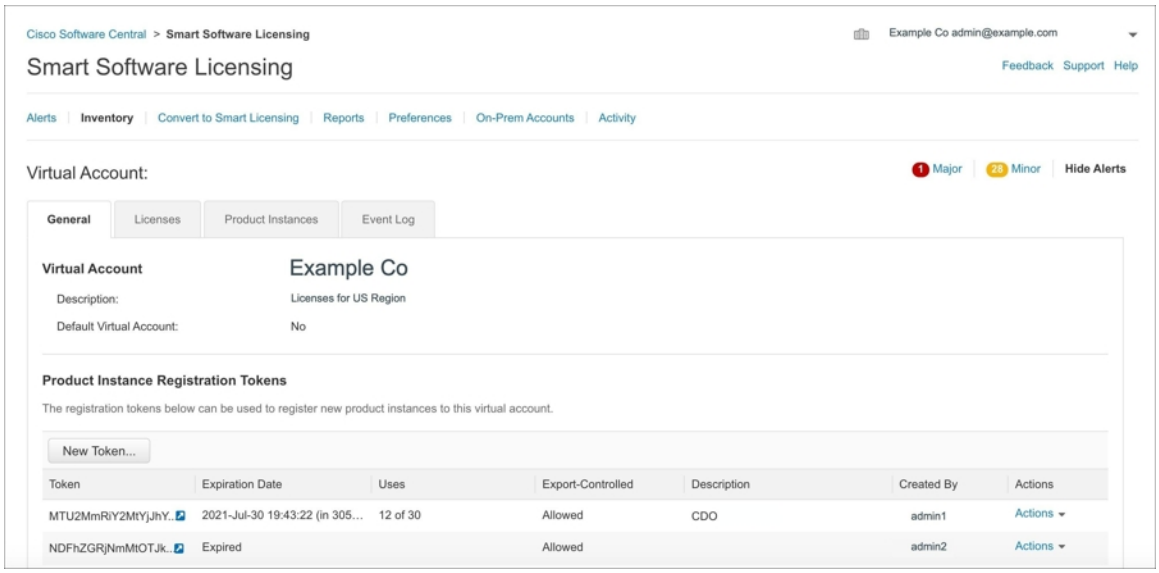
- Smart license an FDM-managed device when onboarding using a registration key.
- Smart license an FDM-managed device after onboarding the device using a registration key or the administrator's credentials.

Note The FDM-managed device may be using a 90-day evaluation license, or the license could be unregistered.

Smart-License an FDM-Managed Device When Onboarding Using a Registration Key

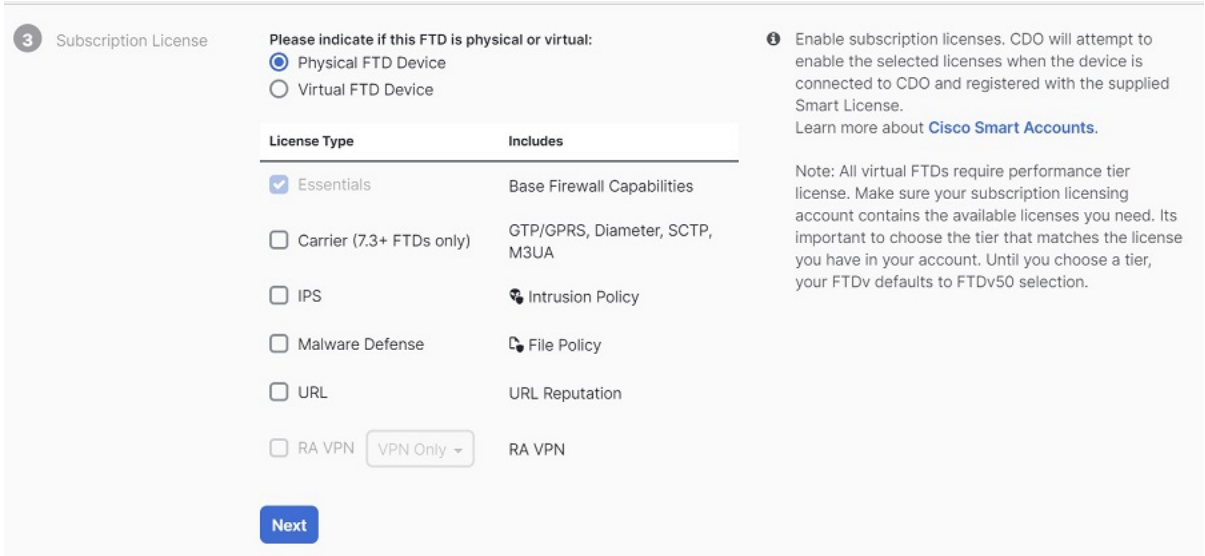
Procedure

Step 1 Log on to the Cisco Smart Software Manager and generate a new Smart License key. Copy the newly generated key. You can watch the Generate Smart Licensing video for more information.



Step 2 Begin onboarding an FDM-managed device using a registration key. For more information, see Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key or Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key.

Step 3 In step 4 of the onboarding wizard, in the **Smart License here** box, paste the Smart License in the **Activate** field and click **Next**.

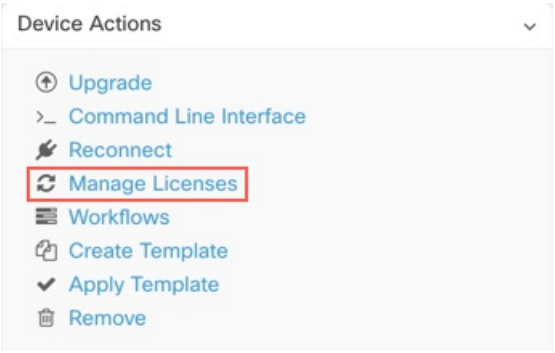


Step 4 Click **Go to Inventory page**.

Step 5 Click the **FTD** tab and see the progress of the onboarding process. The device starts synchronizing and applies the Smart License.

You should see that the device is now in the **Online** connectivity state. If the device is not in the online connectivity state, look in the Device Actions pane on the right and click **Manage Licenses** > **Refresh Licenses** to update the connectivity state.

Step 6 After applying the Smart License successfully to the FDM-managed device, click the **Manage Licenses**. The device status shows "**Connected**, **Sufficient License**." You can enable or disable the optional licenses. For more information, see FDM-Managed Device Licensing Types.



Smart-License an FDM-Managed Device After Onboarding the Device Using a Registration Key or its Credentials

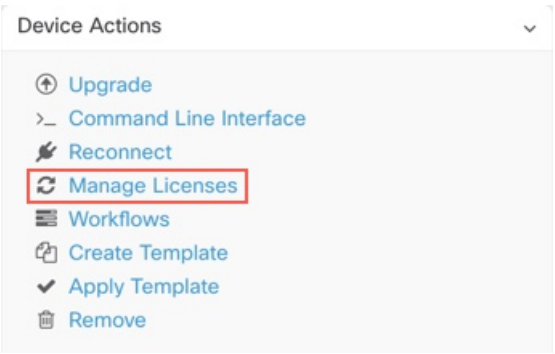
Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device.

Step 3 Click the **FTD** tab and select the device that you want to license.

Step 4 In the **Device Actions** pane on the right, click **Manage Licenses**.



Step 5 Follow the on-screen instructions and enter the Smart License generated from Cisco Smart Software Manager.

Step 6 Paste the new license key in the box and click **Register Device**. After synchronizing with the device, the connectivity state changes to 'Online'. After applying the Smart License successfully to the FDM-managed device, the device status shows "**Connected**, **Sufficient License**." You can enable or disable the optional licenses. For more information, see FDM-Managed Device Licensing Types.

Updating an Existing Smart License of an FDM-Managed Device

You can apply a new Smart License to an FDM-managed device which is Smart Licensed. Based on the method you have selected for onboarding your device, select the appropriate procedure:

Change the Smart License Applied to an FDM-Managed Device Onboarded Using a Registration Key

Procedure

Step 1 Remove the corresponding FDM-managed device from Security Cloud Control.

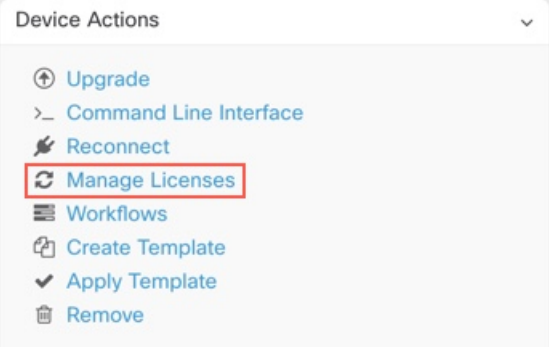
Step 2 Log into the Secure Firewall device manager for that device and unregister the Smart License. For more information, see Unregister a Smart-licensed FDM-Managed Device.

Step 3 In Security Cloud Control, onboard the FDM-managed device again using a registration key. For more information, see Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key.

Step 4 Click the **Devices** tab to locate the device.

Step 5 Click the tab.

Step 6 Apply the new Smart License during the onboarding process or by looking in the **Device Actions** pane on the right and clicking**Manage Licenses**.



Change the Smart License Applied to an FDM-Managed Device Onboarded Using its Credentials

Procedure

Step 1 Log into the Secure Firewall device manager for that device and unregister the Smart License. For more information, see Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key.

Step 2 Apply the new Smart License to the FDM-managed device in Secure Firewall device manager.

a. In the **Smart License** area, click **View Configuration**.

b. Click **Register Now** and follow the onscreen instructions.

Step 3 On the **Inventory** page in Security Cloud Control, click the **Devices** tab.

Step 4 Click the **FTD** device. Check the FDM-managed device configuration for changes so that Security Cloud Control can make a copy of the FDM-managed device's deployed configuration and save it to the Security Cloud Control database. For more information, see About Device Configuration Changes.

Security Cloud Control Support for DHCP Addressing of FDM-Managed Devices

What happens if the IP address used by my FDM-managed device changes?

Security Cloud Control has many Adaptive Security Appliance (ASA) and FDM-managed device customers who have onboarded devices using the IP address provided by their service provider using DHCP.

If the IP address of the device for any reason, whether that is a change in the static IP address or a change in the IP address due to DHCP, you can Changing a Device's IP Address in Security Cloud Control and then reconnect the device.

The field, expressed concerns regarding the case of branch deployed FDM-managed devices managed by Security Cloud Control, a static IP is required on the outside interface of the FDM-managed device, which, in the view of some SE's, precludes using Security Cloud Control as a management solution when the FDM-managed device has a DHCP address configured for the outside interface.

However, this situation does not impact customers that have VPN tunnels to remote branch firewalls, and we know that a vast majority of customers have Site to Site tunnels from their Branch Offices back to their datacenters. In the case that Site-to -Site VPN is used to connect to the central site from devices, DHCP on the outside interface is not a concern since Security Cloud Control (and any management platform) can connect to the FW via its inside, statically addressed, interface (if so configured). This is a recommended practice and we have Security Cloud Control customers with many (+1000) devices using this deployment mode.

Also, the fact that an interface IP address is being issued via DHCP does not preclude the customer from managing the device using that IP. Again, this is not optimal, but the experience of periodically having to potentially change the IP address in Security Cloud Control has not been seen as a hurdle to customers. This situation is not exclusive to Security Cloud Control and happens with any manager using the outside interface including ASDM, FDM or SSH.

FDM-Managed Device Licensing Types

Smart License Types

The following table explains the licenses available for FDM-managed devices.

Your purchase of an FDM-managed device automatically includes a base license. All additional licenses are optional.

License	Duration	Granted Capabilities
License (automatically included)	Perpetual	All features not covered by the subscription term licenses. You must also specify whether to Allow export-controlled functionality on the products registered with this token. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.
	Term-based	**Intrusion detection and prevention**-Intrusion policies analyze network traffic for intrusions and exploits and, optionally, drop offending packets. **File control**-File policies detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types. AMP for Firepower, which requires a Malware license, allows you to inspect and block files that contain malware. You must have the license to use any type of File policy. **Security Intelligence filtering**-Drop selected traffic before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to drop connections based on the latest intelligence immediately.
Malware	Term-based	File policies that check for malware, which use Cisco Advanced Malware Protection (AMP) with AMP for Firepower (network-based Advanced Malware Protection) and Cisco Threat Grid. File policies can detect and block malware in files transmitted over your network.

License	Duration	Granted Capabilities
URL License	Term-based	Category and reputation-based URL filtering. You can perform URL filtering on individual URLs without this license.
	Term-based or perpetual based on the license type	Remote access VPN configuration. Your essentials license must allow export-controlled functionality to configure RA VPN. You select whether you meet export requirements when you register the device. Firepower Device Manager can use any valid AnyConnect license. The available features do not differ based on the license type. If you have not already purchased one, see Licensing Requirements for Remote Access VPN. Also, see the Cisco AnyConnect Ordering Guide, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

Virtual FDM-Managed Device Tiered Licenses

Version 7.0 introduces support for performance-tiered Smart Licensing for virtual FDM-Managed devices based on throughput requirements and RA VPN session limits. When the virtual FDM-Managed device is licensed with one of the available performance licenses, two things occur: session limits for RA VPNs are determined by the installed virtual FDM-Managed device platform entitlement tier, and enforced via a rate limiter.

Security Cloud Control **does not** fully support tiered smart licensing at this time; see the following limitations:

- You cannot modify the tiered license through Security Cloud Control. You must make the changes in the Secure Firewall device manager UI.
- If you register a virtual FDM-Managed device to be managed by the cloud-delivered Firewall Management Center, the tiered license selection automatically resets to **Variable**, which is the default tier.
- If you onboard a virtual FDM-Managed device running version 7.0 or later, and select a license that is **not** a default license during the onboarding process, the tiered license selection automatically resets to **Variable**, which is the default tier.

We strongly recommend selecting a tier for your virtual FDM-Managed device license after onboarding your device to avoid the issues listed above. See Managing Smart Licenses for more information.

Viewing Smart-Licenses for a Device

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select an FDM-managed device to view its current license status.

Step 5 In the **Device Actions** pane on the right, click **Manage Licenses**. The **Manage Licenses** screen provides the following information:

- **Smart License Agent status**: Shows whether you're using a 90-day evaluation license, or if you have registered with the Cisco Smart Software Manager. The Smart License Agent status can be the following:
  - **"Connected," "Sufficient Licenses"** - The device has contacted and registered successfully with the License Authority, which has authorized the license entitlements for the appliance. The device is now In-Compliance.
  - **Out-of-Compliance** - There's no available license entitlement for the device. Licensed features continue to work. However, you can either purchase or free up extra entitlements to become In-Compliance.
  - **Authorization Expired** - The device hasn't communicated with the Licensing Authority in 90 or more days. Licensed features continue to work. In this state, the Smart License Agent retries its authorization requests. If a retry succeeds, the agent enters either an Out-of-Compliance or Authorized state and begins a new Authorization Period. Try manually synchronizing the device.
- **License Registration**: Allows you to apply smart-license to an already onboarded FDM-managed device. Once registered, you can see the status of the connection to the Cisco Smart Software Manager and the status for each type of license.
- **License Status**: Shows the status of the optional licenses available for your FDM-managed device. You can enable a license to use the features controlled by the license.

Enabling or Disabling Optional Licenses

You can enable (register) optional licenses on FDM-managed devices that are using a 90-day evaluation license or a full license. You must enable a license to use the features controlled by the license.

If you no longer want to use the features covered by an optional term license, you can disable (release) the license. Disabling the license releases it in your Cisco Smart Software Manager account so that you can apply it to another device.

In evaluation mode, you can also enable evaluation versions of the optional licenses and perform all operations. In this mode, the licenses aren't registered with Cisco Smart Software Manager until you register the device.

Note You can't enable the license in evaluation mode.

Before you begin

Before disabling a license, ensure that you are not using it. Rewrite or delete any policies that require the license.

For units operating in a high availability configuration, you enable or disable licenses on the active unit only. The change is reflected in the standby unit the next time you deploy the configuration when the standby unit requests (or frees) the necessary licenses. When enabling licenses, you must ensure that your Cisco Smart Software Manager account has sufficient licenses available, or you could have one unit compliant while the other unit is non-compliant.

To enable or disable optional licenses, follow this procedure:

Procedure

Step 1 In the **Inventory** page, select the FDM-managed device that you want and click **Manage Licenses** in **Device Actions pane**, The **Manage Licenses** screen appears.

Step 2 Click the slider control for each optional license to enable or disable the license. The status of the license shows OK when enabled.

- **Enabled**: Registers the license with your Cisco Smart Software Manager account and enable the controlled features. You can now configure and deploy policies controlled by the license.
- **Disabled**: Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.

Step 3 Click **Save** to save the changes.

Impact of Expired or Disabled Optional Licenses

If an optional license expires, you can continue using features that require the license. However, the license is marked out of compliance, and you need to purchase the license and add it to your account to bring the license back into compliance.

If you disable an optional license, the system reacts as follows:

- **Malware license**: The system stops querying the AMP cloud and also stops acknowledging retrospective events sent from the AMP cloud. You cannot re-deploy existing access control policies if they include file policies that apply malware inspection. Note that for a very brief time after a Malware license is disabled, the system can use existing cached file dispositions. After the time window expires, the system assigns a disposition of Unavailable to those files.
- : The system no longer applies intrusion or file-control policies. For Security Intelligence policies, the system no longer applies the policy and stops downloading feed updates. You cannot re-deploy existing policies that require the license.
- **URL**: Access control rules with URL category conditions immediately stop filtering URLs, and the system no longer downloads updates to URL data. You cannot re-deploy existing access control policies if they include rules with category and reputation-based URL conditions.

- : You cannot edit the remote access VPN configuration, but you can remove it. Users can still connect using the RA VPN configuration. However, if you change the device registration so that the system is no longer export compliant, the remote access VPN configuration stops immediately, and no remote users can connect through the VPN.

Create and Import an Firewall Device Manager Model

Security Cloud Control provides the ability to export the complete configuration of an FDM-managed device on a Security Cloud Control tenant to a JSON file format. You can then import this file to another tenant as an Firewall device manager model and apply it to a new device on that tenant. The feature is beneficial when you want to use an FDM-managed device's configuration on different tenants that you manage.

Note If the FDM-managed device contains rulesets, the shared rules associated with the rulesets are modified as local rules when exporting the configuration. Later, when the model is imported to another tenant and applied to an FDM-managed device, you'll see the local rules in the device.

Export FDM-Managed Device Configuration

The export configuration functionality is unavailable if your FDM-managed device has the following configuration:

- High Availability
- Snort 3 enabled

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab.

Step 4 Select an FDM-managed device and in the **Device Actions** on the right pane, click **Export Configuration**.

Import FDM-Managed Device Configuration

Procedure

Step 1 In the **Inventory** page, click the blue plus ( ) button to import the configuration.

Step 2 Click **Import** to import configuration for offline management.

Step 3 Select the **Device Type** as **FTD**.

Step 4 Click **Browse** and select the configuration file (JSON format) to upload.

Step 5 Once the configuration is verified, you're prompted to label the device or service. See Security Cloud Control Labels and Filtering for more information.

Step 6 After labeling your model device, you can view it in the **Inventory** list.

Note Depending on the size of the configuration and the number of other devices or services, it may take some time for the configuration to be analyzed.

Delete a Device from Security Cloud Control

Use the following procedure to delete a device from Security Cloud Control:

Procedure

Step 1 Log into Security Cloud Control.

Step 2 In the left pane, click **Security Devices**.

Step 3 Locate the device you want to delete and check the device in the device row to select it.

Step 4 In the **Device Actions** panel located to the right, select **Remove**.

Step 5 When prompted, select **OK** to confirm the removal of the selected device. Select **Cancel** to keep the device onboarded.

Note that both devices in an FDM-managed HA pair must be deleted simultaenously. Click the FDM-managed HA pair name and not the individual peers.

Import Configuration for Offline Device Management

Importing a device's configuration for offline management allows you to review and optimize a device's configuration without having to work on a live device in your network. Security Cloud Control also refers to these uploaded configuration files as "models."

You can import the configurations of these devices to Security Cloud Control:

- FDM-Managed Device. See Create and Import an Firewall Device Manager Model.
- Cisco IOS devices like the Aggregation Services Routers (ASR) and Integrated Services Routers (ISRs).

Backing Up FDM-Managed Devices

You can use Security Cloud Control to back up an FDM-managed device's system configuration so that you can restore the device to a previous state. Backups include the configuration only, and not the system software. If you need to completely reimage the device, you need to reinstall the software, then you can upload a backup

and recover the configuration. Security Cloud Control saves the last 5 backups made for a device. When a new backup occurs, the oldest backup is deleted in order to store the newest backup.

Note The backup does not include the management IP address configuration. Thus, when you recover a backup file, the management address is not replaced from the backup copy. This ensures that any changes you made to the address are preserved, and also makes it possible to restore the configuration on a different device on a different network segment.

The configuration database is locked during backup. You cannot make configuration changes during a backup, although you can view policies, dashboards, and so forth. During a restore, the system is completely unavailable.

To make backup schedules across your devices consistent, you can configure your own default backup schedule. When you schedule a backup for a particular device, you can use your own default settings or change them. You can schedule recurring backups with cadences from daily to once a month and you can perform an on-demand backup. You can also download backups and then use the Threat Defense device manager to restore them.

Requirements and best practice for backing up and restoring an FDM-managed device using Security Cloud Control

- Security Cloud Control can backup FDM-managed devices running software version 6.5 and later.
- The FDM-managed device must be onboarded to Security Cloud Control using a registration key.
- You can restore a backup onto a replacement device only if the two devices are the same model and are running the same version of the software, including the build number, not just the same point release. For example, a backup of an FDM-managed device running software version 6.6.0-90 can only be restored to an FDM-managed device running 6.6.0-90. Do not use the backup and restore process to copy configurations between appliances. A backup file contains information that uniquely identifies an appliance, so that it cannot be shared in this manner.
- For the Secure Firewall Threat Defense backup functionality to work in Security Cloud Control, threat defense needs to access one of these Security Cloud Control URLs based on your tenant region.
  - edge.apj.cdo.cisco.com
  - edge.aus.cdo.cisco.com
  - edge.eu.cdo.cisco.com
  - edge.in.cdo.cisco.com
  - edge.us.cdo.cisco.com
- Ensure that port 443 has external and outbound access for the HTTPS protocol. If the port is blocked behind a firewall, the backup and restore process may fail.

Best Practice

The device you are going to backup should be in the Synced state in Security Cloud Control. Security Cloud Control backs up the configuration of the device *from the device* not from Security Cloud Control. So, if the device is in a Not Synced state, changes on Security Cloud Control will not be backed up. If the device is in a Conflict Detected state, those changes will be backed up.

Related Information:

Back up an FDM-Managed Device On-Demand

This procedure describes how to backup an FDM-managed device so that it can be restored if need be.

Before you Begin

Review these Backing Up FDM-Managed Devices before you backup up an FDM-managed device.

Procedure

Procedure

Step 1 (Optional) Create a Change Request Management for the backup.

Step 2 In the navigation bar, click **Inventory**.

Step 3 Click the **Devices** tab.

Step 4 Click the **FTD** tab and select the device you want to backup.

Step 5 In the **Device Actions** pane on the right, click **Manage Backups**.

Step 6 Click **Backup Now**. The Device enters the Backing Up configuration state.

When the backup is done, the Security Cloud Control displays the device's configuration state it was in before the backup started. You can also open the change log page to look for a recent change log record with the description, "Backup completed successfully."

If you created a change request in step 1, you can also filter by that value to find the change log entry.

Step 7 if you created a change request in step 1, clear the change request value so you do not inadvertently associated more changes with the change request.

Configure a Recurring Backup Schedule for a Single FDM-Managed Device

Before you Begin

Review these Backing Up FDM-Managed Devices before you backup up an FDM-managed device.

Procedure

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device you want to backup.

Step 4 In the **Device Actions** pane on the right, click **Manage Backups**.

Step 5 In the **Device Backups** page, click **Set Recurring Backup** or click the schedule in the Recurring Backup field. Security Cloud Control presents the default backup schedule for all FDM-managed devices on your tenant. See Configure a Default Recurring Backup Schedule for more information.

Step 6 Select the time of day, in 24-hour time, you want the backup to occur. Note that you schedule the time in Coordinated Universal Time (UTC) time.

Step 7 In the Frequency field, select daily, weekly, or monthly backup.

- Daily backups: Give the scheduled backup a name and a description.
- Weekly backups: Check the days of the week on which you want the backup to occur. Give the scheduled backup time a name and a description.
- Monthly backups: Click in the Days of Month field and add whichever days of the month you want to the schedule the backup. Note: If you enter day 31 but a month doesn't have 31 days in it, the backup will not take place. Give the scheduled backup time a name and a description.

Step 8 Click **Save**. Notice that on the Device Backup page, the Recurring Backup field is replaced by the backup schedule you set and reflects your local time.

Download the Device Backup

This procedure describes how to download a .tar file containing a backup of an FDM-managed device.

Procedure

Step 1 In the navigation bar, click**Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and the device whose backup you want to download.

Step 4 In the Actions pane on the right, click **Manage Backups**.

Step 5 Select the backup you want to download and, in its row, click the **Generate Download Link** button . The button changes to read, "Download Backup Image."

Step 6 The button now reads **Download Backup Image**. Do one of these things:

- If you are on a device that can also reach the Firewall device manager of the device you want to restore, click the**Download Backup Image** button and save the downloaded file. Save it with a name that you will remember.

- If you are not on a device that can also reach the FDM of the device you want to restore:
  a. Right-click the **Download Backup Image** button and copy the link address.

     Important The link address expires 15 minutes after you click the Generate Download Link button.

  b. Open a browser on a device that will also reach the Firewall device manager of the Secure Firewall Threat Defense you want to restore the image to.
  c. Enter the download link into the browser address bar and download the backup file to that device. Save it with a name that you will remember.

Edit a Backup

This procedure allows you to edit the name or description of a successful FDM-managed device download.

Procedure

Step 1 In the navigation bar, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the **FTD** tab and select the device you want to edit.
Step 4 In the Actions pane on the right, click **Manage Backups**.
Step 5 Select the backup you want to edit and it's row, click the edit icon .
Step 6 Change the name or description of the backup. You can see the new information in the Device Backups page.

Delete a Backup

Security Cloud Control saves the last 5 backups made for a device. When a new backup occurs, the oldest backup is deleted in order to store the newest backup. Deleting existing backups may help you manage which backups are kept and which are deleted.

Procedure

Step 1 In the navigation bar, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the **FTD** tab and select the device you want to delete.
Step 4 In the Actions pane on the right, click **Manage Backups**.
Step 5 Select the backup you want to delete and it's row, click the trash icon .

Step 6 Click **OK** to confirm.

Managing Device Backup

Backups of FDM-managed devices you produce using Security Cloud Control can be seen in the Device Backups page:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab.

Step 4 Click the filter icon and check FDM under Devices/Services to see only FDM-managed devices in the device table.

Step 5 Select the device you want.

Step 6 In the **Device Actions** pane, click **Manage Backups**. You will see up to 5 of the latest backups made of that device.

What to do next

See Restore a Backup to an FDM-Managed Device, on page 207 if you want to restore a backup.

Restore a Backup to an FDM-Managed Device

Review this information before you restore a backup of an FDM-managed managed threat defense device.

- Review these Backing Up FDM-Managed Devices before you restore a backup to an FDM-managed threat defense device.
- If the backup copy you want to restore is not already on the device, you must **upload** the backup first before restoring it.
- During a restore, the system is completely unavailable. After the backup is restored, the device reboots.
- This procedure assumes that you have an existing backup of the device ready to be restored to the device.
- You cannot restore a backup if the device is part of a high availability pair. You must first break HA from the Device > High Availability page, then you can restore the backup. If the backup includes the HA configuration, the device will rejoin the HA group. Do not restore the same backup on both units, because they would then both go active. Instead, restore the backup on the unit you want to go active first, then restore the equivalent backup on the other unit.

Note The backup does not include the management IP address configuration. Thus, when you recover a backup file, the management address is not replaced from the backup copy. This ensures that any changes you made to the address are preserved, and also makes it possible to restore the configuration on a different device on a different network segment.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device you want to restore.

Step 4 In the **Device Actions** pane on the right, click **Manage Backups**.

Step 5 Select the backup you want to restore. In its row, click the **Generate Download Link** button .

Note The link address expires 15 minutes after you click the Generate Download Link button.

Step 6 The button now reads **Download Backup Image**. Do one of these things:

- If you are on a device that can also reach the Firewall device manager of the device you want to restore, click the **Download Backup Image**button and save the downloaded file. *Save it with a name that you will remember*.
- If you are not on a device that can also reach the firewall device manager of the device you want to restore:
  - **a.** Right-click the **Download Backup Image** button and copy the link address.
  - **b.** Open a browser on a device that will also reach the firewall device manager you want to restore the image to.
  - **c.** Enter the download link into the browser address bar and download the backup file to that device. *Save it with a name that you will remember*.

Step 7 Log on to Firewall device manager for the device you want to restore.

Step 8 Open version 6.5 or higher of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager. Navigate to the System Management chapter, and search for **Restoring a Backup**. Follow those instructions to restore the image you just downloaded to your FDM-managed device.

Tip You will need to upload your image to firewall device manager in order to restore it.

Step 9 Follow the prompts in firewall device manager. When the restore starts, your browser is disconnected from firewall device manager. After the restore has finished, the device reboots.

Related Information:

- Backing Up FDM-Managed Devices
- Back up an FDM-Managed Device On-Demand

- Configure a Recurring Backup Schedule for a Single FDM-Managed Device
- Download the Device Backup
- Edit a Backup

FDM Software Upgrade Paths

Upgrading FDM Versions

If you use Security Cloud Control to upgrade your FDM-managed firewalls, Security Cloud Control determines which version you can upgrade to and you will not need this topic. If you maintain your own repository of FDM images and upgrade your FDM-managed devices using your own images, this topic explains what upgrade paths are available to you.

You can upgrade an FDM-managed device directly from one major or maintenance version to another; for example, Version 6.4.0 > 6.5.0, or Version 6.4.0 > 7.0.1. You do not need to be running any specific patch level.

If direct upgrade is not possible, your upgrade path must include intermediate versions, such as Version 6.4.0 > 7.0.0 > 7.1.0.

Table 9: Upgrade Paths for Major Releases

Target Version	Oldest Release you can Upgrade to the Target Version
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

Patching FDM-Managed Devices

You cannot upgrade directly from a patch of one version to a patch of another version, such as from Version 6.4.0.1 > 6.5.0.1. You must upgrade to the major release first, and then patch that release. For example you must upgrade from Version 6.4.0.1 > 6.5.0 > 6.5.0.1.

Firepower Hotfixes

Security Cloud Control does not support hotfix updates or installations. If there is a hotfix available for your device model or software version, we strongly recommend using the configured manager's dashboard or UI. After a hotfix is installed on the device, Security Cloud Control detects out of band configuration changes.

Removing FDM Upgrades

You cannot use Security Cloud Control to remove or downgrade any release type, whether major, maintenance, or patch.

Starting with Secure Firewall Threat Defense defense Version 6.7.0, you can use Firepower Device Manager or the FTD CLI to revert a successfully upgraded device to its state just before the last major or maintenance upgrade (also called a snapshot). Reverting after patching necessarily removes patches as well. After reverting, you must reapply any configuration changes you made between **upgrading** and reverting. **Note that to revert a major or maintenance upgrade to FDM Version 6.5.0 through 6.6.x, you must reimage.** See the "System Management" section of a Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for more information.

Removing FDM Patches

You cannot remove an FDM patch with either Security Cloud Control or FDM. To remove a patch, you must reimage to a major or maintenance release.

Snort Upgrade

Snort is the main inspection engine for the product and is packaged into the Secure Firewall Threat Defense software for your convenience. Version 6.7 introduces an update to the package that you can upgrade to, or revert from, at any time. Although you can switch Snort versions freely, some intrusion rules in Snort 2.0 might not exist in Snort 3.0, and vice versa. We strongly recommend reading about the differences in the Firepower Device Manager Configuration Guide for Version 6.7.0 for more information.

To proceed with upgrading your FDM-managed device to use Snort 3 or to revert from Snort 3 back to Snort 2 from the Security Cloud Control UI, see Upgrade to Snort 3.0 and Revert From Snort 3.0 for FDM-Managed Device respectively.

Other Upgrade Limitations

2100 Series Devices

Security Cloud Control can upgrade Firepower 2100 series devices only if they are running appliance mode.

- Firepower Threat Defense devices are always in appliance mode.

What to do next

See the "Cisco Firepower 2100 Getting Started Guide" for a more detailed discussion of these commands.

4100 and 9300 Series Devices

Security Cloud Control does not support the upgrade for the 4100 or 9300 series devices. You must upgrade these devices outside of Security Cloud Control.

Related Information:

- FDM-Managed Device Upgrade Prerequisites
- Upgrade a Single FDM-Managed Device
- Bulk FDM-Managed Devices Upgrade

- Upgrade an FDM-Managed High Availability Pair

FDM-Managed Device Upgrade Prerequisites

Security Cloud Control provides a wizard that helps you upgrade the Firewall device manager (FDM) images installed on an individual device or an HA pair.

The wizard guides you through the process of choosing compatible images, installs them, and reboots the device to complete the upgrade. We secure the upgrade process by validating that the images you chose on Security Cloud Control are the ones copied to, and installed on, your FDM-managed device. We strongly recommend the FDM-managed devices you are upgrading have outbound access to the internet.

If your FDM-managed device does not have outbound access to the internet, you can download the image you want from Cisco.com, store them in your own repository, provide the upgrade wizard with a custom URL to those images, and Security Cloud Control performs upgrades using those images. In this case, however, you determine what images you want to upgrade to. Security Cloud Control does not perform the image integrity check or disk-space check.

Configuration Prerequisites

- DNS needs to be enabled on the FDM-managed device. See the "Configuring DNS" section of the **System Administration** chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running for more information.
- The FDM-managed device should be able to reach the internet if you use upgrade images from Security Cloud Control's image repository.
- The FDM-managed device has been successfully onboarded to Security Cloud Control.
- The FDM-managed device is reachable.
- The FDM-managed device is synced.
    - If you update a device that has pending changes in Security Cloud Control and you do not accept changes, pending changes are lost after the upgrade completes. Best practice is to deploy any pending changes before you upgrade..
    - If you have staged changes in firewall device manager and the device is not synced, the upgrade in Security Cloud Control will fail at an eligibility check.

4100 and 9300 Series Running FTD

Security Cloud Control does not support the upgrade for the 4100 or 9300 series devices. You must upgrade these devices outside of Security Cloud Control.

Software and Hardware Requirements

Security Cloud Control is a cloud management platform. Software updates are released over time and are generally not dependent on hardware. See Devices, Software, and Hardware Supported by Security Cloud Control for information about supported hardware types.

Devices running firewall device manager software have a recommended upgrade path for optimal performance. See FDM Software Upgrade Paths for more information.

Upgrade Notes

You cannot deploy changes to a device while it is upgrading.

Related Information:

- FDM Software Upgrade Paths
- Upgrade a Single FDM-Managed Device
- Bulk FDM-Managed Devices Upgrade
- Upgrade an FDM-Managed High Availability Pair

Upgrade a Single FDM-Managed Device

Before You Begin

Be sure to read through the FDM-Managed Device Upgrade Prerequisites, FDM Software Upgrade Paths, and the Devices, Software, and Hardware Supported by Security Cloud Control before you upgrade. This document covers any requirements and warnings you should know prior to upgrading to your desired version of Firepower software.

Upgrade A Single FDM-Managed Device with Images from Security Cloud Control's Repository

Use the following procedure to upgrade a standalone FDM-managed device using a software image that is stored in Security Cloud Control's repository:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device..

Step 3 Click the **FTD** tab.

Step 4 Select the device you want to upgrade.

Step 5 In the **Device Actions** pane, click **Upgrade**.

Step 6 In step 1, click **Use Security Cloud Control Image Repository** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.

Step 7 In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.

Step 8 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 9 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 10 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control.

Step 11 Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4in for more information.

Upgrade a Single FDM-Managed Device with Images from your own Repository

Use the following procedure to upgrade a standalone FDM-managed device using a URL protocol to locate a software image:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device..

Step 3 Click the **FTD** tab.

Step 4 Select the device you want to upgrade.

Step 5 In the **Device Actions** pane, click **Upgrade**.

Step 6 In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.

Step 7 In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.

Step 8 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 9 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 10 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control.

Step 11 Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4in for more information.

Monitor the Upgrade Process

You can view the progress of your single device by selecting that device on the **Inventory** page and clicking the upgrade button. Security Cloud Control takes you to the Device Upgrade page for that device.

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information

Bulk FDM-Managed Devices Upgrade

Before You Begin

Be sure to read through the FDM-Managed Device Upgrade Prerequisites, FDM Software Upgrade Paths,and the Devices, Software, and Hardware Supported by Security Cloud Control before you upgrade. This document covers any requirements and warnings you should know prior to upgrading to your desired version of Firepower software.

Note You can only bulk upgrade FDM-managed devices if they are all upgrading to the same software version.

Upgrade Bulk FDM-Managed Devices with Images from Security Cloud Control's Repository

Use the following procedure to upgrade multiple FDM-managed devices using a software image that is stored in Security Cloud Control's repository:

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate your devices.

Step 3 Click the **FTD** tab.

Step 4 Use the Filters to narrow down the list of devices you may want to include in your bulk upgrade.

Step 5 From the filtered list of devices, select the devices you want to upgrade.

Step 6 In the **Device Actions** pane, click **Upgrade**.

Step 7 On the Bulk Device Upgrade page, the devices that can be upgraded are presented to you. If any of the devices you chose are not upgradable, Security Cloud Control gives you a link to view the not upgradable devices.

Step 8 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 9 In step 1, click **Use Security Cloud Control Image Repository** to select the software image you want to upgrade to. You are only presented with choices that are compatible with the devices you can upgrade. Click **Continue**.

Step 10 In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.

Step 11 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrades while in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrades after it has started, Security Cloud Control does not deploy or poll for changes from the devices. Devices do not roll back to the previous configuration after a canceled upgrade, either. This may cause the devices to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 12 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to theMonitor Jobs in Security Cloud Control.

Step 13 Upgrade the system databases. You must do this step in Firewall device manager. See **Updating System Databases** in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, for the version your device is running.

Upgrade Bulk FDM-Managed Devices with Images from your own Repository

Use the following procedure to upgrade multiple FDM-managed devices using a URL protocol to locate a software image:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your devices.

Step 3 Click the **FTD** tab.

Step 4 Use the Filters to narrow down the list of devices you may want to include in your bulk upgrade.

Step 5 From the filtered list of devices, select the devices you want to upgrade.

Step 6 In the **Device Actions** pane, click **Upgrade**.

Step 7 On the Bulk Device Upgrade page, the devices that can be upgraded are presented to you. If any of the devices you chose are not upgradable, Security Cloud Control gives you a link to view the not upgradable devices.

Step 8 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 9 In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**.

Step 10 In step 2, confirm your choices and decide whether you only want to download the images to your devices or copy the images, install them, and reboot the device.

Step 11 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrades while in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrades after it has started, Security Cloud Control does not deploy or poll for changes from the devices and the devices do not roll back to the previous configuration. This may cause the devices to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 12 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control.

Step 13 Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4 in for more information.

Monitor the Bulk Upgrade Process

You can view the progress of a single device that was included in the bulk upgrade by selecting that device on the **Inventory** page and clicking the upgrade button. You can also view the progress details by clicking **Jobs** in the left pane and expanding the bulk operation.

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.

Upgrade an FDM-Managed High Availability Pair

Upgrade your HA pair without disrupting traffic; the standby device continues to handle traffic detection while the secondary device is upgraded.

When you upgrade an HA pair, Security Cloud Control executes an eligibility check and copies or identifies the image location before starting the upgrade. The secondary device in a high availability pair upgrades first, even if it is currently the active device; if the secondary device is the Security Cloud Control active device, the paired devices automatically switch roles for the upgrade process. Once the secondary devices successfully upgrade, the devices switch roles, then the new standby device upgrades. When the upgrade completes, the devices are automatically configured so the primary device is active and the secondary device is standby.

We do not recommend deploying to the HA pair during the upgrade process.

Before You Begin

- Deploy all pending changes to the active device before upgrading.

- Ensure there are no tasks running during the upgrade.
- Both devices in the HA pair are healthy.
- Confirm you are ready to upgrade; you cannot rollback to a previous version in Security Cloud Control.
- Read through the FDM-Managed Device Upgrade Prerequisites, FDM Software Upgrade Paths, and the Devices, Software, and Hardware Supported by Security Cloud Control to review any requirements and warnings that may incur during the ugprade process.

Upgrade an FDM-Managed HA Pair with Images from Security Cloud Control's Repository

Use the following procedure to upgrade an FDM-managed HA pair using a software image that is stored in Security Cloud Control's repository:

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select the HA pair you want to upgrade.

Step 5 In the **Device Actions** pane, click **Upgrade**.

Step 6 In step 1, click **Use Security Cloud Control Image Repository** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.

Step 7 In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.

Step 8 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or poll changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 9 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 10 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control.

Step 11 Upgrade the system databases. You must do this step in FDM. See "Updating System Databases" in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4 in for more information.

Upgrade an FDM-Managed HA Pair with Images from your own Repository

Use the following procedure to upgrade an FDM-managed HA pair using a URL protocol to locate a software image:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select the HA pair you want to upgrade.

Step 5 In the **Device Actions** pane, click **Upgrade**.

Step 6 In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.

Step 7 In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.

Step 8 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or poll changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 9 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 10 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control.

Step 11 Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4 for more information.

Monitor the Upgrade Process

You can view the progress of your single device by selecting that device on the **Inventory** page and clicking the upgrade button. Security Cloud Control takes you to the **Device Upgrade** page for that device.

During the upgrade, the system suspends HA while updating system libraries, which includes an automatic deployment, and may not be in a healthy state for the entirety of the upgrade process. This is expected. The device is available for SSH connections during the last part of this process, so if you log in shortly after applying an upgrade, you might see HA in suspended status. If the system experiences issues during the upgrade process and the HA pair appears to be suspended, manually resume HA from the Firewall device manager console of the active device.

Note If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Upgrade to Snort 3.0

Snort 3 is the latest snort engine, or a powerful preprocessor that uses Open Source Intrusion Prevention System (IPS), available for Firepower Version 6.7 and later. The snort engine uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users and is ideally used as a packet sniffer, a packet logger, or, more traditionally, as a a standalone network IPS.

With Snort 3, you can now create custom intrusion policies; every FDM-managed device running Snort 3 has a set of intrusion policies that are pre-defined from Cisco's Talos Intelligence Group (Talos). Snort 3 makes it possible to change these default policies, although we strongly recommend building on top of the base for a more robust policy.

You cannot create custom policies with Snort 2.

Switching from Snort 2 to Snort 3

You can switch Snort versions freely, though some intrusion rules in Snort 2.0 might not exist in Snort 3.0, and vice versa. If you changed the rule action for an existing rule, that change is not preserved if you switch to Snort 3 and then back to Snort 2, or back again to Snort 3. Your changes to rule actions for rules that exist in both versions are preserved. Note that the mapping between rules in Snort 3 and Snort 2 can be one-to-one or one-to-many, so preservation of changes is done on a best-effort basis.

If you choose to upgrade from Snort 2 to Snort 3, please note that upgrading the snort engines is comparable to a system upgrade. We strongly recommend upgrading during a maintenance window to minimize the interruption in traffic monitoring for your network. See Managing Intrusion Policies (Snort3) in the *Firepower Device Manager Configuration Guide* as to how switching snort versions will affect how rules process traffic.

Tip You can filter by Snort version on the **Inventory** page, and the Details window of a selected device displays the current version running on the device.

Snort 3 Limitations

License Requirements

To allow the snort engine to process traffic for intrusion and malware analysis, you must have the **license** enabled for the FDM-managed device. To enable this license through Firewall device manager, log into the Firewall device manager UI and navigate to **Device** > **View Configuration** > **Enable/Disable** and enable the license.

Hardware Support

The following devices support Snort 3:

- FTD 1000 series
- FTD 2100 series
- FTD 4100 series
- FTD virutal with AWS
- FTD virtual with Azure
- ASA 5500-X Series with FTD

Software Support

Devices **must** be running at least Firewall device manager Version 6.7. Security Cloud Control supports Snort 3 functionality for devices running Version 6.7 and later.

For FTD 1000 and 2000 series, see FXOS bundled support for more information on FXOS patch support.

Configuration Limitations

Security Cloud Control does not support upgrading to Snort 3 if your device has the following configurations:

- Device is not running at least Version 6.7.
- If a device has pending changes. Deploy any changes prior to upgrading.
- If a device is currently upgrading. Do not attempt to upgrade or deploy to the device until the device is synced.
- If a device is configured with a virtual router.

Note If you upgrade or revert the Snort version, the system automatically deploys to implement the changes between Snort 2 intrusion policies and Snort 3 intrusion policies.

Rulesets and Snort 3

Note that Snort 3 does not have full feature support at this time. Security Cloud Control rulesets are not supported on Snort 3 devices. If you simultaneously upgrade a device to Firewall device manager 6.7 or higher, and from Snort 2 to Snort 3, any rulesets configured prior to the upgrade are broken up and the rules in them are saved as individual rules.

For a full list of ruleset support in regards to devices configured for Snort 3, see Rulesets, on page 393.

Upgrade the Device and the Intrusion Prevention Engine Simultaneously

Security Cloud Control allows you to upgrade the device to Version 6.7 and the Snort 3. Use the following procedure to upgrade the FDM-managed device:

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device or devices you want to upgrade.

Step 4 In the **Devices Actions** pane located to the right, click **Upgrade**.

Step 5 Set the upgrade toggle to **FTD System Upgrade**.

Step 6 (Optional) If you want Security Cloud Control to perform the upgrade later, check the **Schedule Upgrade** check box. Click in the field to select a date and time in the future.

Step 7 In step 1, select your upgrade method. Either use the Security Cloud Control Image Repository and an image from your own repository:

- **Use Security Cloud Control Image Repository** - Click this option to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- **Specify Image URL** - Click this option to select the software image that is currently stored in your own repository, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.

Step 8 In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.

Step 9 Check **Upgrade to Snort 3 Engine**.

Step 10 Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Upgrade the Intrusion Prevention Engine

For devices that are already running Version 6.7 with Snort 2, use the following procedure to update just the Snort engine to version 3:

Procedure

Step 1 In the navigation bar, click **Inventory**.

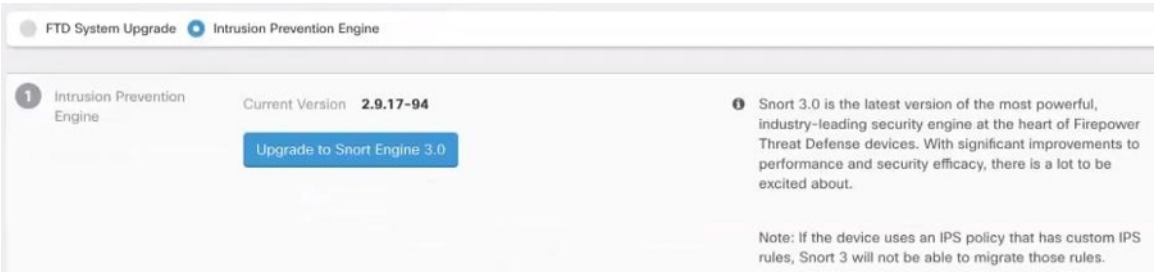
Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device or devices you want to upgrade.

Step 4 In the **Device Actions** pane located to the right, click **Upgrade**.

Step 5 Set the upgrade toggle to **Intrusion Prevention Engine**.

Step 6 Click **Upgrade to Snort Engine 3.0**.



Step 7 From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Monitor the Upgrade Process

Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

You can view the progress of your single device by selecting that device on the **Inventory** page and clicking the upgrade button. Security Cloud Control takes you to the **Device Upgrade** page for that device.

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information

Revert From Snort 3.0 for FDM-Managed Device

Some intrusion rules in Snort 2.0 might not exist in Snort 3.0. If you downgrade to 2.0, any custom intrusion policies that you created are converted to the base policy used in the custom policy. As far as possible, rule action overrides are retained. If more than one custom policy uses the same base policy, the overrides of the custom policy that is used in the most access control policies are retained, and the overrides for the other custom policies are lost. Access control rules that used these"duplicate"policies will now use the base policy created from your most-used custom policy. All custom policies are deleted.

Before you opt to revert from Snort 3.0, read Managing Intrusion Policies (Snort2) of the *Firepower Device Manager Configuration Guide* and find out how switching snort engine versions will affect your current rules and policies.

Note Reverting to version 2 does not uninstall the Firepower software version.

Revert From Snort 3.0

If you change the Snort version,the system will perform an automatic deployment to implement the change. Note that you can only revert individual devices from Snort 3.0 to version 2.

Use the following procedure to revert the intrusion prevention engine:

Procedure

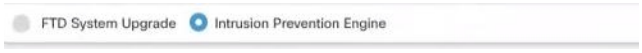
Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

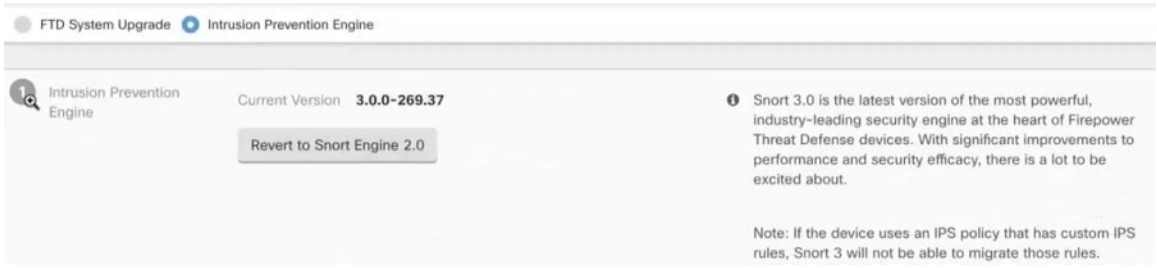
Step 3 Click the **FTD** tab and and click the device you want to revert.

Step 4 In the **Device Actions** pane located to the right, click **Upgrade**.

Step 5 Set the upgrade toggle to **Intrusion Prevention Engine**.



Step 6 In Step 1, confirm you want to revert from Snort version 3, and click **Revert to Snort Engine 2**.



Step 7 From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Schedule a Security Database Update

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the desired FDM-managed device.

Step 4 In the Actions pane, locate the **Security Database Updates** section and click the add + button.

Note If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

Step 5 Configure the scheduled task with the following:

- **Frequency** - Choose for the update to occur daily, weekly, or monthly.
- **Time** - Choose the time of day. Note that the time displayed is UTC.
- **Select Days** - Choose which day(s) of the week you want the update to occur.

Step 6 Click **Save**.

Step 7 The device's Configuration Status will change to "Updating Databases".

Edit a Scheduled Security Database Update

Use the following procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the desired FDM-managed device.

Step 4 In the Actions pane, locate the **Database Updates** section and click the edit icon.

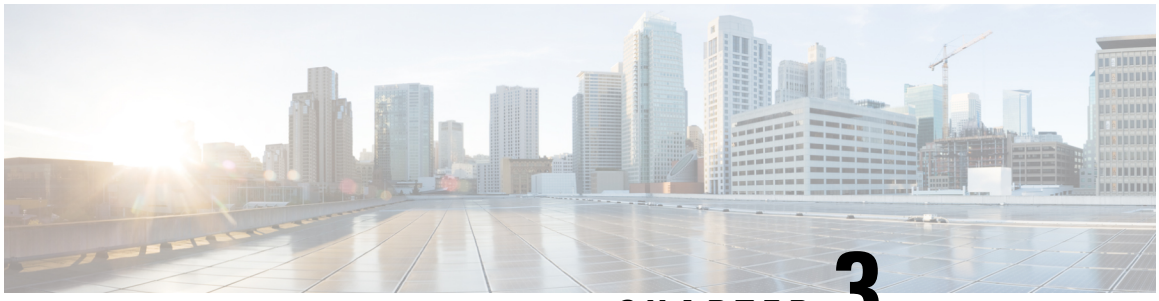
Step 5 Edit the scheduled task with the following:

- **Frequency** - Choose for the update to occur daily, weekly, or monthly.

- **Time** - Choose the time of day. Note that the time displayed is UTC.
- **Select Days** - Choose which day(s) of the week you want the update to occur.

Step 6 Click **Save**.

Step 7 The device's Configuration Status will change to "Updating Databases".



CHAPTER 3

Configuring FDM-Managed Devices

- Schedule a Security Database Update, on page 581
- Update FDM-Managed Device Security Databases, on page 582

Interfaces

You can use Security Cloud Control to configure and edit data interfaces or the management/diagnostic interface on an FDM-managed device.

At this time, Security Cloud Control can only configure routed interfaces and bridge groups. It does not support the configuration passive interfaces.

Guidelines and Limitations for Firepower Interface Configuration

When you use Security Cloud Control to configure the device, there are several limitations to interface configuration. If you need any of the following features, you must use Firepower Management Center to configure the device.

Firewall

- Routed firewall mode only is supported. You cannot configure transparent firewall mode interfaces.
- Only physical firepower 1010 devices support interfaces configured for switch port mode. See Switch Port Mode Interfaces for an FDM-Managed Device for more information.

Passive

- At this time, Security Cloud Control does not identify passive interface mode in the interface table ad you cannot configure passive or ERSPAN interfaces. You must use the FDM-managed UI to configure and identify passive interfaces.

IPS-Only Mode

- You cannot configure interfaces to be inline (in an inline set), or inline tap, for IPS-only processing. IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. In comparison, Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization.
- Optionally, you can configure IPS functions for this firewall mode traffic according to your security policy.

EtherChannel

Security Cloud Control supports read, create, and abilities for devices running Version 6.5 and later. To create Etherchannel interfaces, see Add an EtherChannel Interface for an FDM-Managed Device for more information. To create

- You can configure up to 48 EtherChannels on physical Firepower devices, although how many interfaces can be active at a time depends on your device model. For device-specific limitations, see Device-Specific Limitations.

- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.
- The device to which you connect the EtherChannel must also support 802.3ad EtherChannels.
- The FDM-managed device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS vlan dot1Q tag native command, then the FDM-managed device will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.
- All FDM-managed device configuration refers to the logical EtherChannel interface instead of the member physical interfaces.

Note Interfaces set up as portchannels can only use physical interfaces, redundant interfaces, and subinterfaces are supported as bridge group member interfaces.

Bridge Groups

At this time, Security Cloud Control supports the configuration of one bridge group. To determine if your device supports bridge groups, see Bridge Group Compatibility in FDM-Managed Configurations for more information.

When adding an interface to a bridge group, keep the following in mind:

- The interface must have a name.
- The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP.
- BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
- BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
- The interface cannot be Point-to-Point Protocol over Ethernet (PPPoE)
- The interface cannot be associated with a security zone (if it is in a zone). You must delete any NAT rules for the interface before you can add it to a bridge group.
- Enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.
- You can configure the interfaces that will be ***members*** of the bridge group. See Configure a Bridge Group for interface requirements and creation.

Point-to-Point Protocol over Ethernet

- You cannot configure Point-to-Point Protocol over Ethernet (PPPoE) for IPv4. If the Internet interface is connected to a DSL, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address, you must use the FDM to configure these settings.

VLAN

To configure VLAN interfaces and VLAN members, see Configure an FDM-Managed Device VLAN for more information. To configure VLAN for switch port mode, see Configure an FDM-Managed Device VLAN for Switch Port Mode for more information.

- The interface must be physical.
- The interface cannot be management-only.
- The interface cannot be associated as any other type of interface, including BVI, subinterfaces, another VLAN interface, EtherChannel, etc.
- The interface cannot be a BVI member or an etherchannel member.
- Device models support varying numbers of VLAN members. See Maximum Number of VLAN Members by Device Model for more information.

Note To configure VLAN for your environment, see Configure Firepower VLAN Subinterfaces and 802.1Q Trunking for more information.

Network Module Cards

Optional network module installations are limited to the ASA 5515-X, 5525-X, 5545-X, and 5555-X, and the Firepower 2100 series devices.

- Cards are only discovered during bootstrap (that is, initial installation or reimage, or when switching between local/remove management). Security Cloud Control sets the correct defaults for speed and duplex for these interfaces. If you replace an optional card with one that changes the speed/duplex options for the interfaces, without changing the total number of interfaces available, reboot the device so that the system recognizes the correct speed/duplex values for the replaced interfaces. From an SSH or Console session with the device, enter the reboot command. Then, using Security Cloud Control, edit each physical interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.
- You cannot enable or disable network modules or perform breakout online insertion and removal (OIR) of interfaces on FDM-managed Secure Firewall 3100 series devices.

Note Replacing a card with one that changes the total number of interfaces, or removing interfaces that were referred to by other objects, can result in unexpected problems. If you need to make this kind of change, please first remove all references to the interfaces you will remove, such as security zone membership, VPN connections, and so forth. We also suggest you do a backup prior to making the change.

Interfaces on Virtual FDM-Managed Devices

- You cannot add or remove interfaces without reinitializing a virtual FDM-managed device. You must execute these actions in an FDM-managed device.

Note If you replace interfaces with ones that have different speed/duplex capabilities, reboot the device so that the system recognizes the new speed/duplex values with the following procedure: from the device's CLI console, enter the reboot command. Then, in Security Cloud Control, edit each interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.

Maximum Number of VLAN Members by Device Model

The device model limits the maximum number of VLAN subinterfaces that you can configure. Note that you can configure subinterfaces on data interfaces only, you cannot configure them on the management interface. The following table explains the limits for each device model.

Model	Maximum VLAN Subinterfaces
Firepower 1010	60
Firepower 1120	512
Firepower 1140, Firepower 1150	1024
Firepower 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	100

Firepower Data Interfaces

Security Cloud Control supports configuring routed interfaces and bridge virtual interfaces on FDM-managed devices.

Routed Interfaces

Each Layer 3 routed interface (or subinterface) requires an IP address on a unique subnet. You would typically attach these interfaces to switches, a port on another router, or to an ISP/WAN gateway.

You can assign a static address, or you can obtain one from a DHCP server. However, if the DHCP server provides an address on the same subnet as a statically-defined interface on the device, the system will disable the DHCP interface. If an interface that uses DHCP to get an address stops passing traffic, check whether the address overlaps the subnet for another interface on the device.

You can configure both IPv6 and IPv4 addresses on a routed interface. Make sure you configure a default route for both IPv4 and IPv6. This task will need to be performed on the FDM-managed device using Firepower Device Manager. See "Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version x.x.x", **The Basics > Routing** for information about configuring a default route.

Bridge Groups and Bridge Virtual Interfaces

A bridge group is a group of interfaces that the FDM-managed device bridges instead of routes. Bridged interfaces belong to a bridge group, and all interfaces are on the same network. The bridge group is represented by a Bridge Virtual Interface (BVI) that has an IP address on the bridge network. Interfaces included in the bridge group are called "members."

You can route between routed interfaces and BVIs, if you name the BVI. In this case, the BVI acts as the gateway between member interfaces and routed interfaces. If you do not name the BVI, traffic on the bridge group member interfaces cannot leave the bridge group. Normally, you would name the interface so that you can route member interfaces to the Internet.

FDM-managed devices only support one bridge group, therefore, Security Cloud Control can only manage that one bridge group and cannot create additional bridge groups on the device. Security Cloud Control can only manage BVIs on FDM-managed devices installed directly on hardware, not on virtual FDM-managed device instances.

One use for a bridge group in routed mode is to use extra interfaces on the FDM-managed device instead of an external switch. You can attach endpoints directly to bridge group member interfaces. You can also attach switches to add more endpoints to the same network as the BVI.

Passive Interfaces

Passive interfaces monitor traffic flowing across a network using a switch SPAN (Switched Port Analyzer) or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

At this time, Security Cloud Control has limited support for managing passive interfaces on the FDM-managed device:

- Passive interfaces must be configured on the FDM-managed device.
- Routed interfaces cannot be changed to passive interfaces and passives interfaces cannot be changed to routed interfaces using Security Cloud Control.
- Security Cloud Control does not identify passive interfaces in the interface table.

Related Information:

- IPv6 Addressing for Firepower Interfaces

- Guidelines and Limitations for Firepower Interface Configuration
- Configure a Physical Firepower Interface

Management/Diagnostic Interface

The physical port labeled Management (or for FDM-managed device virtual, the Management 0/0 virtual interface) actually has two separate interfaces associated with it.

- **Management virtual interface**-This IP address is used for system communication. This is the address the system uses for Smart Licensing and to retrieve database updates. You can open management sessions to it (Firepower Device Manager and CLI). You must configure a management address, which is defined on **System Settings** > **Management Interface**.
- **Diagnostic physical interface**-The physical Management port is actually named Diagnostic. You can use this interface to send syslog messages to an external syslog server. Configuring an IP address for the Diagnostic physical interface is optional. The only reason to configure the interface is if you want to use it for syslog. This interface appears, and is configurable, on the **Inventory** > **Interfaces** page. The Diagnostic physical interface only allows management traffic, and does not allow through traffic.

(Hardware devices.) The recommended way to configure Management/Diagnostic is to not wire the physical port to a network. Instead, configure the Management IP address only, and configure it to use the data interfaces as the gateway for obtaining updates from the Internet. Then, open the inside interfaces to HTTPS/SSH traffic (by default, HTTPS is enabled) and open Firepower Device Manager using the inside IP address. This task you must perform on Firepower Device Manager directly. See "Configuring the Management Access List" in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for instructions.

For FDM-managed device virtual, the recommended configuration is to attach Management0/0 to the same network as the inside interface, and use the inside interface as the gateway. Do not configure a separate address for Diagnostic.

Note **For special instructions on how to edit the Management interface see** Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for Firepower version 6.4 or higher. Open the guide and navigate to **The Basic** > **Interfaces** > **Management/Diagnostic Interface**. Management interface configuration should be done on the Firepower Device Manager.

Interface Settings

Use these topics to configure interface settings.

Use of Security Zones in Firepower Interface Settings

Each interface can be assigned to a single security zone. You then apply your security policy based on zones. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. You can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside, for example.

Each zone has a mode, either routed or passive. This relates directly to the interface mode. You can add routed and passive interfaces only to the same mode security zone.

Bridge Virtual Interfaces (BVIs) are not added to security zones. Only member interfaces are added to security zones.

You do not include the Diagnostic or Management interface in a zone. Zones apply to data interfaces only.

Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores VTI interfaces. If a security zone or static route references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference. Security Cloud Control support for VTI tunnels is coming soon.

See Security Zone Object for more information about security zones.

Assign an FDM-Managed Device Interface to a Security Zone

Before you Begin

An interface has the following limitations when adding a security zone:

- The interface must have a name.
- The interface cannot be management-only. This option is enabled and disabled from the Advanced tab of the interface.
- You cannot assign a security zone to a bridge group interface.
- You cannot assign a security zone to an interface configured for switchport mode.
- Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores VTI interfaces. If a security zone or static route references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference. Security Cloud Control support for VTI tunnels is coming soon.

Assign a Firepower Interface to a Security Zone

Use the following procedure to associate a security zone to an existing interface:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** device and select the FDM-managed device you want to modify.

Step 4 In the **Management** pane located to the right, click **Interfaces**.

Step 5 Select the interface you want to add a security zone to and click **Edit**.

Step 6 Use the **Security Zone** drop-down menu and select the security zone you want associated with this interface.

Note If need to, ceate a new security zone from this drop-down menu by clicking **Create New**.

Step 7 Click **Save**.

Step 8 Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device.

Related Information:

- Security Zone Object
- Create or Edit a Firepower Security Zone Object
- Guidelines and Limitations for Firepower Interface Configuration

Use of Auto-MDI/MDX in Firepower Interface Settings

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

These settings are configured on the Advanced tab when editing an interface.

Use of MAC Addresses in Firepower Interface Settings

You can manually configure Media Access Control (MAC) addresses to override the default value.

For a high availability configuration, you can configure both the active and standby MAC address for an interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption.

Active and standby MAC addresses are configured on the Advanced tab when configuring an interface.

Default MAC Addresses

Default MAC address assignments depend on the type of interface.

- **Physical interfaces** - The physical interface uses the burned-in MAC address.
- **Subinterfaces** - All subinterfaces of a physical interface use the same burned-in MAC address. You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses.

Use of MTU Settings in Firepower Interface Settings

About the MTU

The MTU specifies the maximum frame payload size that the FDM-managed device can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Path MTU Discovery

The FDM-managed device supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so they can standardize on the lowest MTU in the path.

MTU and Fragmentation

For IPv4, if an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. For IPv6, packets are typically not allowed to be fragmented at all. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

For UDP or ICMP, the application should take the MTU into account to avoid fragmentation.

Note The FDM-managed device can receive frames larger than the configured MTU as long as there is room in memory.

MTU and Jumbo Frames

A larger MTU lets you send larger packets. Larger packets might be more efficient for your network. See the following guidelines:

- Matching MTUs on the traffic path: We recommend that you set the MTU on all FDM-managed device interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames: A jumbo frame is an Ethernet packet larger than the standard maximum of 1522 bytes (including Layer 2 header and VLAN header), up to 9216 bytes. You can set the MTU up to 9198 bytes to accommodate jumbo frames. The maximum is 9000 for FDM-managed virtual.

Note Increasing the MTU assigns more memory for jumbo frames, which might limit the maximum usage of other features, such as access rules. If you increase the MTU above the default 1500 on ASA 5500-X series devices or FDM-managed virtual, you must reboot the system. You do not need to reboot Firepower 2100 series devices, where jumbo frame support is always enabled.

Jumbo frame support is enabled by default on Firepower 3100 devices.

IPv6 Addressing for Firepower Interfaces

You can configure two types of unicast IPv6 addresses for Firepower physical interfaces.

- **Global**—The global address is a public address that you can use on the public network. For a bridge group, you configure the global address on the Bridge Virtual Interface (BVI), not on each member interface. You cannot specify any of the following as a global address.
  - Internally reserved IPv6 addresses: fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - An unspecified address, such as ::/128

- The loopback address, ::1/128
- Multicast addresses, ff00::/8
- Link-local addresses, fe80::/10

- **Link-local**—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the Network Discovery functions such as address resolution and neighbor discovery. Each interface must have its own address because the link-local address is only available on a segment, and is tied to the interface MAC address.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Configuring Firepower Interfaces

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for traffic to pass through it. If the interface is a member of a bridge group, naming the interface is sufficient. If the interface is a bridge virtual interface (BVI), you need to assign the BVI an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs.

The interface list shows the available interfaces, their names, addresses, and states. You can change the state of an interface, on or off, or edit an interface, by selecting the interface row and clicking **Edit** in the Actions pane. The list shows the interface characteristics based on your configuration. Expand an interface row to see subinterfaces or bridge group member.

Related Information:

- Interfaces
- Configure a Physical Firepower Interface
- Configure Advanced Firepower Interface Options, on page 245
- Configure Firepower VLAN Subinterfaces and 802.1Q Trunking
- Configure an FDM-Managed Device VLAN for Switch Port Mode

Configure a Physical Firepower Interface

At a minimum, you must enable a physical interface to use it. You would also typically name it and configure IP addressing; however, you would not configure IP addressing if you intend to create VLAN subinterfaces, if you are configuring a passive mode interface, or if you intend to add the interface to a bridge group.

Note You cannot configure IP addresses on bridge group member interfaces or passive interfaces, although you can modify advanced settings, that are not related to IPv6 addressing.

You can disable an interface to temporarily prevent transmission on the connected network. You do not need to remove the interface's configuration. At this time, Security Cloud Control can only configure routed interfaces and bridge groups. Security Cloud Control lists passive interfaces but you cannot reconfigure them as active interfaces from Security Cloud Control.

Note **Note**: Security Cloud Control does not support Point-to-Point Protocol over Ethernet (PPPoE) configurations for IPv4. Configuring this option in an FDM-managed devicemay cause isses in the Security Cloud Control UI; if you **must** configure PPPoE for your device, you must make the appropriate changes in an FDM-managed device.

Procedure

Procedure

Step 1 In the left pane, click **Security Devices** and click the device whose interfaces you want to configure and click **Interfaces** in the **Management** pane on the right.

Step 2 On the **Interfaces** page, select the physical interface you want to configure.

Step 3 In the **Actions** pane on the right, click **Edit**.

Step 4 Give the physical interface a **Logical Name** and, optionally, a **Description**. Unless you configure subinterfaces, the interface should have a name.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

Step 5 Pick one of these options:

- If you intend to add sub-interfaces:

If you intend to configure subinterfaces for this physical interface, you are probably done. Click **Save** and continue with Configure Firepower VLAN Subinterfaces and 802.1Q Trunking ; otherwise, continue.

Note Even when configuring subinterfaces, it is valid to name the interface and supply IP addresses. This is not the typical setup, but if you know that is what you need, you can configure it.

- If you do not intend to add a sub-interface, continue with either or both, Configure IPv4 Addressing for the Physical Interface and Configure IPv6 Addressing for the Physical Interface.

Configure IPv4 Addressing for the Physical Interface

Warning After you configure and save a DHCP address pool, the DHCP address pool is bound to the interface's configured IP address(es). If you edit the interface's subnet mask after you configure a DHCP address pool, deployments to the FDM-managed device fail. Also, if you edit the DHCP address pool in the FDM-managed console and read the configuration from an FDM-managed device to Security Cloud Control, the read fails.

Procedure

Step 1 In the "Editing Physical Interface" dialog, click the **IPv4 Address** tab.

Step 2 Select one of the following options from the Type field:

- **Static**-Choose this option if you want to assign an address that should not change. Enter in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address you enter is not the network ID or the broadcast address for the network and the address is not already used on the network.
  - **Standby IP Address and Subnet Mask** - If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
  - **(Optional) DHCP Address Pool** - Enter a a single DHCP Server IP address, or an IP address range. The range of IP addresses must be on the same subnet as the selected interface and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address. Specify the start and end address for the pool, separated by a hyphen. To temporarily disable this DHCP server, edit the server in the **DHCP Servers** section of the Configure DHCP Servers page.
- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. Change the following options if necessary:
  - **Obtain Default Route**-Whether to get the default route from the DHCP server. You would normally check this option.
  - **DHCP Route Metric**-If you obtain the default route from the DHCP server, enter the administrative distance to the learned route, between 1 and 255.

    Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes.

Step 3 Click **Save** if you are done or continue with one of these procedures:

- Configure IPv6 Addressing for the Physical Interface if you intend to assign an IPv6 address to this interface as well as an IPv4 address.
- Configure Advanced Firepower Interface Options, on page 245. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure IPv6 Addressing for the Physical Interface

Procedure

Step 1 In the "Editing Physical Interface" dialog, click the IPv6 Address tab.

Step 2 **State**-To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

Step 3 **Address Auto Configuration**-Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the FDM-managed device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

Step 4 **Suppress RA**-Check this box if you want to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the Firepower Threat Defense device to supply the IPv6 prefix (for example, the outside interface).

Step 5 **Link-Local Address**-If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

Step 6 **Standby Link-Local Address**-Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other FDM-managed device, to which this interfaces is connected.

Step 7 **Static Address/Prefix**â€”If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing for Firepower Interfaces.

Step 8 **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 9 Click **Save** if you are done or continue with one of these procedures:

- Configure Advanced Firepower Interface Options, on page 245. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Enable the Physical Interface

Procedure

Step 1 Select the interface you want to enable.

Step 2 Slide the **State** slider at the top right of the window, associated with the interface's logical name to blue.

Step 3 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Firepower VLAN Subinterfaces and 802.1Q Trunking

VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.

Note You cannot configure IP addresses on bridge group member interfaces, although you can modify advanced settings as needed.

Before You Begin

Prevent untagged packets on the physical interface. If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterface to pass traffic, ensure that the physical interface

does not pass traffic by not naming the interface. If you want to let the physical interface pass untagged packets, you can name the interface as usual.

Procedure

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and click the device whose interfaces you want to configure.

Step 4 Click **Interfaces** in the **Management** pane at the right.

Step 5 On the Interfaces page, select the physical interface you want to configure and in the Actions pane at the right, click **+ New Subinterface**.

Notice that the **Parent Interface** field shows the name of the physical interface for which you are creating this subinterface. You cannot change the parent interface after you create the subinterface.

Step 6 Give the subinterface a **logical name** and, optionally, a **description**. Without a logical name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

Step 7 Configure the VLAN ID and Subinterface ID:

- **VLAN ID** - Enter a VLAN ID between 1 and 4094 that will be used to tag the packets on this subinterface.
- **Subinterface ID** - Enter the subinterface ID as an integer between 1 and 4294967295. The number of subinterfaces allowed Maximum Number of VLAN Members by Device Model. You cannot change the subinterace ID after you create the subinterface.

Continue with Configure IPv4 Addressing for the Subinterface and Configure IPv6 Addressing for the Subinterface .

Configure IPv4 Addressing for the Subinterface

Procedure

Step 1 In the "Adding Subinterface" dialog, click the **IPv4 Address** tab.

Step 2 Select one of the following options from the Type field:

- **Static**-Choose this option if you want to assign an address that should not change.

  Enter in the interface's **IP address and the subnet mask** for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the

address you enter is not the network ID or the broadcast address for the network and the address is not already used on the network.

- Enter a **Standby IP Address** and Subnet Mask only if this interface is being used in a high availability pair of devices.
- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. Change the following options if necessary:
  - **Obtain Default Route**-Whether to get the default route from the DHCP server. You would normally check this option.
  - **DHCP Route Metric**-If you obtain the default route from the DHCP server, enter the administrative distance to the learned route, between 1 and 255.

  See Configure DHCP Servers.

  Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes.

Step 3 Click **Create** if you are done or continue with one of these procedures:

- Continue to "Configure IPv6 Addressing for the Physical Interface" if you want to assign an IPv6 address to this interface as well as an IPv4 address.
- Configure Advanced Firepower Interface Options, on page 245. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you created the subinterface, go to Enable the Physical Interface .

Configure IPv6 Addressing for the Subinterface

Procedure

Step 1 Click the IPv6 Address tab.

Step 2 **Enable IPv6 processing**-To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, move the **State** slider to blue. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

Step 3 **Address Auto Configuration**-Check this option to have the address automatically configured. IPv6 stateless auto configuration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Step 4 **Suppress RA**-Check this box if you want to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the Firepower Threat Defense device to supply the IPv6 prefix (for example, the outside interface).

Step 5 **Link-Local Address**-If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

Step 6 **Standby Link-Local Address**-Configure this address if your interface connects a high availability pair of devices.

Step 7 **Static Address/Prefix**-If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing, on page 136.

Step 8 **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 9 Click **Create** if you are done or continue with one of these procedures:

- Click the Advanced tab to Configure Advanced Firepower Interface Options, on page 245. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you created the subinterface, go to Enable the Physical Interface .

Enable the Physical Interface

Procedure

Step 1 To enable the subinterface, slide the State slider, associated with the subinterface's logical name to blue.

Step 2 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Advanced Firepower Interface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Limitations:

- You cannot set MTU, duplex, or speed for the Management interface on a Firepower 2100 series device.
- The MTU of an unnamed interface **must** be set to 1500 bytes.

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and click the device whose interfaces you want to configure.

Step 4 Click **Interfaces** in the **Management** pane at the right.

Step 5 On the Interfaces page, select the physical interface you want to configure and in the Actions pane at the right, click **Edit**.

Step 6 Click the **Advanced** tab.

Step 7 **Enable for HA Monitoring** is automatically enabled. When this is enabled, the device includes the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.

Step 8 To make a data interface management only, check **Management Only**.

A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.

Step 9 Modify the IPv6 DHCP configuration settings.

- **Enable DHCP for IPv6 address configuration** - Whether to set the Managed Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.
- **Enable DHCP for IPv6 non-address configuration** - Whether to set the Other Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

Step 10 Configure **DAD Attempts** - How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

Step 11 Change the MTU (maximum transmission unit) to the desired value.

The default MTU is 1500 bytes. You can specify a value from 64 - 9198 (or 9000, for Firepower Threat Defense Virtual). Set a high value if you typically see jumbo frames on your network. See Use of MTU Settings in Firepower Interface Settings for more information.

Note If you increase MTU above 1500 on ASA 5500-X series devices, ISA 3000 series devices, or Firepower Threat Defense Virtual, you must reboot the device. Log into the CLI and use the reboot command. You do not need to reboot the Firepower 2100 or Secure Firewall 3100 series devices, where jumbo frame support is always enabled.

Step 12 (Physical interface only.) Modify the **speed** and **duplex** settings.

The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. The options listed are only those supported by the interface. Before setting these options for interfaces on a network module, please read Guidelines and Limitations for Firepower Interface Configuration.

- **Duplex**- Choose Auto , Half , Full , or Default . Auto is the default when the interface supports it. For example, you cannot select Auto for the SFP interfaces on a Firepower 2100 or Secure Firewall 3100 series device. Select Default to indicate that Firepower Device Manager should not attempt to configure the setting.

  Any existing configuration is left unchanged.

- **Speed**- Choose Auto to have the interface negotiate the speed (this is the default), or pick a specific speed: 10 , 100 , 1000 , 10000 Mbps. You can also select these special options:

  Any existing configuration is left unchanged.

  The type of interface limits the options you can select. For example, the SFP+ interfaces on a Firepower 2100 series device support 1000 (1 Gbps) and 10000 (10 Gpbs) only, and the SFP interfaces support 1000 (1 Gbps) only, whereas GigabitEthernet ports do not support 10000 (10 Gpbs). SPF interfaces on other devices might require No Negotiate . Consult the hardware documentation for information on what the interfaces support.

Step 13 (Optional, recommended for subinterfaces and high availability units.) Configure the MAC address.

MAC Address-The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)

Standby MAC Address-For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 14 Click **Create**.

Configure a Bridge Group

A bridge group is a virtual interface that groups one or more interfaces. The main reason to group interfaces is to create a group of switched interfaces. Thus, you can attach workstations or other endpoint devices directly to the interfaces included in the bridge group. You do not need to connect them through a separate physical switch, although you can also attach a switch to a bridge group member.

The group members do not have IP addresses. Instead, all member interfaces share the IP address of the Bridge Virtual Interface (BVI). If you enable IPv6 on the BVI, member interfaces are automatically assigned unique link-local addresses.

You typically configure a DHCP server on the bridge group interface (BVI), which provides IP addresses for any endpoints connected through member interfaces. However, you can configure static addresses on the endpoints connected to the member interfaces if you prefer. All endpoints within the bridge group must have IP addresses on the same subnet as the bridge group IP address.

Note For ISA 3000, the device comes pre-configured with bridge group BVI, named inside, which includes all data interfaces except for the outside interface. Thus, the device is pre-configured with one port used for linking to the Internet or other upstream network, and all other ports enabled and available for direct connections to endpoints. If you want to use an inside interface for a new subnet, you must first remove the needed interfaces from BVI.

FDM-managed devices only support one bridge group; therefore, Security Cloud Control can only manage that one bridge group and cannot create additional bridge groups on the device.

After you create a bridge group on Security Cloud Control, you will not know the bridge group ID until after the configuration is deployed to the FDM-managed device. FDM-managed device assigns the bridge group ID, for example, BVI1. If the interface is deleted and a new bridge group is created, the new bridge group receives an incremented number, for example, BVI2.

Before you Begin

Configure the interfaces that will be ***members*** of the bridge group. Specifically, each ***member*** interface must meet the following requirements:

- The interface must have a name.
- The interface cannot be configured as **management-only**.
- The interface cannot be configured for passive mode.
- The interface cannot be an EtherChannel interface or an EtherChannel subinterface.
- The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP. If you need to remove the address from an interface that you are currently using, you might also need to remove other configurations for the interface, such as static routes, DHCP server, or NAT rules, that depend on the interface having an address. If you try to add an interface with an IP address to a bridge group, Security Cloud Control will warn you. If you continue to add the interface to the bridge group, Security Cloud Control will remove the IP address from the interface configuration.
- BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
- The interface cannot be Point-to-Point Protocol over Ethernet (PPPoE)
- The interface cannot be associated with a security zone (if it is in a zone). You must delete any NAT rules for the interface before you can add it to a bridge group.
- Enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.
- Bridge groups do not support clustering.

Note Bridge groups are not supported on Firepower 2100 devices in routed mode or on VMware with bridged ixgbevf interfaces.

Configure the Name of the Bridge Group Interface and Select the Bridge Group Members

In this procedure you give the bridge group interface (BVI) a name and select the interfaces to add to the bridge group:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to create a bridge group.

Step 4 Do one of the following:

- Select the BVI bridge group and click **Edit** in the Actions pane.
- Click the plus button and select Bridge Group Interface.

Note You can create and configure a single bridge group. If you already have a bridge group defined, you should edit that group instead of trying to create a new one. If you need to create a new bridge group, you must first delete the existing bridge group.

Step 5 Configure the following:

- **Logical Name**-You must give the bridge group a name. It can be up to 48 characters. Alphabetic characters must be lower case. For example, inside or outside. Without a name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

- (Optional) **Description**-The description can be up to 200 characters on a single line, without carriage returns.

Step 6 Click the **Bridge Group Member** tab. A bridge group can have up to 64 interfaces or subinterfaces to a single bridge group.

- Check an interface to add it to the bridge group.
- Uncheck an interface you want to remove from the bridge group.

Step 7 Click **Save**.

The BVI now has a name and member interfaces. Continue with the following tasks to configure the bridge group interface. You are not performing these tasks for the member interfaces themselves:

- Configure the IPv4 Address for the BVI if you are assigning an IPv4 address to the BVI.
- Configure the IPv6 Address for the BVI if you are assigning an IPv6 address to the BVI.
- Configure Advanced Interface Options for the bridge group interface.

Configure the IPv4 Address for the BVI

Procedure

Step 1 Select the device for which you want to create a bridge group.

Step 2 Select the BVI in the list of interfaces and click **Edit** in the Actions pane.

Step 3 Click the IPv4 Address tab to configure the IPv4 address.

Step 4 Select one of the following options from the Type field:

- **Static**-Choose this option if you want to assign an address that should not change. Type in the bridge group's IP address and the subnet mask. All attached endpoints will be on this network. For models with a pre-configured bridge group, the default for the BVI "inside" network is 192.168.1.1/24 (i.e. 255.255.255.0). Ensure that the address is not already used on the network.

  If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

  Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See Configuring DHCP Server.

- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. This is not the typical option for bridge groups, but you can configure it if needed. You cannot use this option if you configure high availability. Change the following options if necessary:
  - Route Metricâ€”If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
  - Obtain Default Routeâ€”Check this option to get the default route from the DHCP server. You would normally select this option, which is the default.

Step 5 Continue with one of the following procedures:

- Configure the IPv6 Address for the BVI if you are assigning an IPv4 address to the BVI.
- Configure Advanced Interface Options.

- Click **Save** and deploy the changes to the Firepower device. See Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device for more information.

Configure the IPv6 Address for the BVI

Procedure

Step 1 Click the IPv6 Address tab to configure IPv6 addressing for the BVI.

Step 2 Configure these aspects of IPv6 addressing:

Step 3 **Enable IPv6 processing**-To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, slide the **State** slider to blue. The link local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

Step 4 **Suppress RA**-Whether to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately auto-configure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FDM-managed device to supply the IPv6 prefix (for example, the outside interface).

Step 5 **Static Address/Prefix**-If you do not use stateless auto configuration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing.

Step 6 **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 7 Continue with one of the following procedures:

- Configure Advanced Interface Options.
- Click **Save** and deploy the changes to the Firepower device. See Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device for more information.

Configure Advanced Interface Options

You configure most advanced options on bridge group ***member*** interfaces, but some are available for the bridge group interface itself.

Procedure

Step 1 The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 2 Click **OK**.

Step 3 Click **Save** and deploy the changes to the Firepower device. See Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device for more information.

What to do next

- Ensure that all member interfaces that you intend to use are enabled.
- Configure a DHCP server for the bridge group. See Configure DHCP Servers.
- Add the member interfaces to the appropriate security zones.
- Ensure that policies, such as identity, NAT, and access, supply the required services for the bridge group and member interfaces.

Bridge Group Compatibility in FDM-Managed Configurations

In various configurations, where you can specify an interface, sometimes you will be able to specify a bridge virtual interface (BVI) and sometimes you will be able to specify a member of the bridge group. This table explains when a BVI can be used and when a member interface can be used.

Firepower Threat Defense Configuration Type	BVI can be used	BVI member can be used
DHCP server	Yes	No
DNS Server	Yes	Yes
Management access	Yes	No
NAT (Network Address Translation)	No	Yes
Security Zone	No	Yes
Site-to-Site VPN access point	No	Yes
Syslog Server	Yes	No

Delete a Bridge Group

When you delete a bridge group, its members become standard routed interfaces, and any NAT rules or security zone membership are retained. You can edit the interfaces to give them IP addresses. If you need to create a new bridge group, you must first delete the existing bridge group.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device from which you want to delete the bridge group.

Step 4 Select the BVI bridge group and click **Remove** in the Actions pane.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Add an EtherChannel Interface for an FDM-Managed Device

EtherChannel Interface Limitations

An EtherChannel, depending on the device model, can include multiple member interfaces of the same media type and capacity and must be set to the same speed and duplex. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

EtherChannel interfaces have a number of limitations based on physical configuration and software versions. See the sections below for more information.

General Interface Limitations

- EtherChannels are only available on devices running FDM-managed Version 6.5 and later.
- Security Cloud Control supports EtherChannel interface configuration on the following Firepower devices: 1010, 1120, 1140, 1150, 2110, 2120, 2130, 2140, 3110, 3120, 3130, and 3140. For interface limitations per device model, see Device-Specific Limitations.
- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.
- The device to which you connect the EtherChannel must also support 802.3ad EtherChannels.
- The FDM-managed device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS vlan dot1Q tag native command, then the FDM-managed device will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.
- All FDM-managed device configuration refers to the logical EtherChannel interface instead of the member physical interfaces.
- Portchannel interfaces are displayed as physical interfaces.

Device-Specific Limitations

The following devices have specific interface limitations:

1000 Series

- Firepower 1010 supports up to 8 EtherChannel interfaces.
- Firepower 1120,1140,1150 supports up to 12 EtherChannel interfaces.
- 1000 series do not support LACP rate fast; LACP always uses the normal rate. This setting is not configurable.

2100 Series

- Firepower 2110 and 2120 models supports up to 12 EtherChannel interfaces.
- Firepower 2130 and 2140 models support up to 16 EtherChannel interfaces.
- 2100 series do not support LACP fast rate; LACP always uses the normal rate. This setting is not configurable.

Secure Firewall 3100 Series

- All Secure Firewall 3100 models support up to 16 EtherChannel interfaces.
- The Secure Firewall 3100 models support LACP fast rate.
- The Secure Firewall 3100 series models do not support enabling or disabling of network modules and breakout online insertion and removal (OIR) of interfaces.

4100 Series and 9300 Series

- You cannot create or configure EtherChannels on the 4100 and 9300 series. Etherchannels for these devices must be configured in the FXOS chassis.
- Etherchannels on the 4100 and 9300 series appear in Security Cloud Control as physical interfaces.

Add an EtherChannel Interface

Use the following procedure to add an EtherChannel to your FDM-managed device:

Note If you want to immediately create another EtherChannel, check the **Create another** checkbox and then click **Create**.

Procedure

Step 1 Click the **Devices** tab.

Step 2 Click the **FTD** tab and select the device you want to add an EtherChannel to.

Step 3 In the **Management** pane located to the right, select **Interfaces**.

Step 4 Click the blue plus button and select **EtherChannel**.

Step 5 (Optional) Enter a **Logical Name**.

Step 6 (Optional) Enter a description.

Step 7 Enter the **EtherChannel ID**.

For Firepower 1010 series, enter a value between 1 and 8.

For the Firepower 2100, 3100, 4100, and 9300 series, enter a value between 1 and 48.

Step 8 Click the drop-down button for **Link Aggregation Control Protocol** and select one of the two options:

- **Active** - Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **On** - The EtherChannel is always on, and LACP is not used. An **on** EtherChannel can only establish a connection with another EtherChannel that is also configured to be **on**.

Step 9 Search for and select the interfaces you want to include in the EtherChannel as memebers. You **must** include at least one interface.

Warning: If you add an EtherChannel interface as a member and it already has an IP address configured, Security Cloud Control removes the IP address of the member.

Step 10 Click **Create**.

Related Information:

- Edit Or Remove an EtherChannel Interface for FDM-Managed Device
- Add a Subinterface to an EtherChannel Interface
- Edit or Remove a Subinterface from an EtherChannel
- Guidelines and Limitations for Firepower Interface Configuration
- Assign an FDM-Managed Device Interface to a Security Zone
- Add an EtherChannel Interface for an FDM-Managed Device, on page 252

Edit Or Remove an EtherChannel Interface for FDM-Managed Device

Use the following procedures to either modify an existing EtherChannel interface, or remove an EtherChannel interface from an FDM-managed device.

Edit an EtherChannel

Note that EtherChannels have several limitations you must be aware of when modifying. See EtherChannel for more information.

Note EtherChannels must have at least one member.

Use the following procedure to edit an existing EtherChannel:

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the threat defense associated with the Etherchannel you want to modify.

Step 4 In the **Management** pane located to the right, click **Interfaces**.

Step 5 On the **Interfaces** page, select the EtherChannel interface you want to edit. In the Actions pane located to the right, click the edit icon  .

Step 6 Modify any of the following items:

- Logical name.
- State.
- Description.
- Security Zone assignment.
- Link Aggregation Control Protocol status.
- IP address configuration in either the **IPv4**, **IPv6**, or **Advanced** tabs.
- EtherChannel members.

Warning If you add an EtherChannel interface as a member and it already has an IP address configured, Security Cloud Control removes the IP address of the member.

Step 7 Click **Save**.

Remove an EtherChannel Interface

Note EtherChannel interfaces associated with a high availability (HA) or any other configuration. You must manually remove the EtherChannel interface from all configurations before deleting it from Security Cloud Control.

Use the following procedure to remove an EtherChannel interface from an FDM-managed device:

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and the threat defense associated with the Etherchannel you want to delete.

Step 4 In the **Management** pane located to the right, select **Interfaces**.

Step 5 On the **Interfaces** page, select the EtherChannel interface you want to edit. In the Actions pane located to the right, click **Remove**.

Step 6 Confirm you want to delete the EtherChannel interface and click **OK**.

Add a Subinterface to an EtherChannel Interface

EtherChannel Subinterfaces

The **Interfaces** page allows you to view which interfaces of a device have subinterfaces by expanding each interface. This expanded view also shows you the unique logical name, enabled/disabled state, any associated security zones, and mode of the subinterface. The interface type and mode of the subinterface is determined by the parent interface.

General Limitations

Security Cloud Control does not support subinterfaces for the following interface types:

- Interface configured for management-only.
- Interface configured for switch port mode.
- Passive interfaces.
- VLAN interfaces.
- Bridge virtual interfaces (BVI).
- Interfaces that are already a member of another EtherChannel interface.

You **can** create subinterfaces for the following:

- Bridge group members.
- EtherChannel interfaces.
- Physical interfaces.

Add a Subinterface to an EtherChannel Interface

Use the following procedure to add a subinterface to an existing interface:

Note If you want to immediately create another subinterface, check the **Create another** checkbox and then click **Create**.

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the threat defense you want to add an EtherChannel to. In the Management pane located to the right, select **Interfaces**.

Step 4 Select the interface you want to group the subinterface under. In the Action pane located to the right, click the + New Subinterface button.

Step 5 (Optional) Enter a **Logical Name**.

Step 6 (Optional) Enter a description.

Step 7 (Optional) Assign a security zone to the subinterface. Note that you cannot assign a security zone if the subinterface does not have a logical name.

Step 8 Enter a VLAN ID.

Step 9 Enter the **EtherChannel ID**. Use a value between 1 and 48; use values between 1 and 8 for the Firepower 1010 series.

Step 10 Select the **IPv4**, **IPv6**, or **Advanced** tab to configure the IP address of the subinterface.

Step 11 Click **Create**.

Edit or Remove a Subinterface from an EtherChannel

Use the following procedures to either modify an existing subinterface, or remove a subinterface from an Etherchannel interface.

Note Subinterfaces and EtherChannel interfaces have a series of guidelines and limitations that may affect your configuration. See the General Limitations for more information.

Edit a Subinterface

Use the following procedure to edit an existing subinterface associated with an EtherChannel interface:

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the threat defense associated with the EtherChannel and subinterface you want to edit.

Step 4 In the **Management** pane located to the right, select **Interfaces**.

Step 5 Locate and expand the Etherchannel interface that the subinterface is a member of.

Step 6 Select the desired subinterface you want to edit. In the Action pane located to the right, click the edit icon .

Step 7 Modify any of the following items:

- Logical name.
- State.

- Description.
- Security Zone assignment.
- VLAN ID
- IP address configuration in either the IPv4, IPv6, or Advanced tabs.

Step 8 Click **Save**.

Remove a Subinterface from an EtherChannel

Use the following procedure to remove an existing subinterface from an EtherChannel interface:

Procedure

Step 1 In the navigation pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the **FTD** tab and select the threat defense associated with the EtherChannel and subinterface you want to edit. In the Management pane located to the right, select **Interfaces**.
Step 4 Locate and expand the Etherchannel interface that the subinterface is a member of.
Step 5 Select the desired subinterface you want to delete.
Step 6 In the Actions pane located to the right, click **Remove**.
Step 7 Confirm you want to delete the subinterface interface and click **OK**.

Add Interfaces to a Virtual FDM-Managed Device

When you deploy a virtual FDM-managed device, you assign interfaces to the virtual machine. Then, from within an FDM-managed device, you configure those interfaces using the same methods you would use for a hardware device.

However, you cannot add more virtual interfaces to the virtual machine and then have FDM automatically recognize them. If you need more physical-interface equivalents for a virtual FDM-managed device, you basically have to start over. You can either deploy a new virtual machine, or you can use the following procedure.

Caution Adding interfaces to a virtual machine requires that you completely wipe out the virtual FDM-managedconfiguration. The only part of the configuration that remains intact is the management address and gateway settings.

Before You Begin

Do the following in an FDM-managed device:

- Examine the virtual FDM-managed device configuration and make notes on settings that you will want to replicate in the new virtual machine.

- Select **Devices** > **Smart License** > **View Configuration** and disable all feature licenses.

Procedure

Step 1 Power off the virtual FDM-managed device.

Step 2 Using the virtual machine software, add the interfaces to the virtual FDM-managed device. For VMware, virtual appliances use e1000 (1 Gbit/s) interfaces by default. You can also use vmxnet3 or ixgbe (10 Gbit/s) interfaces

Step 3 Power on the virtual FDM-managed device.

Step 4 Open the virtual FDM-managed device console, delete the local manager, then enable the local manager. Deleting the local manager, then enabling it, resets the device configuration and gets the system to recognize the new interfaces. The management interface configuration does not get reset. The following SSH session shows the commands.

```
> show managers
Managed locally.
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager. Otherwise, those licenses remain assigned to the device
 in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
> show managers
No managers configured.
> configure manager local
>
```

Step 5 Open a browser session to an FDM-managed device, complete the device setup wizard, and configure the device. See the "Complete the Initial Configuration" section of the Getting Started chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version x.x.x, guide for more instructions.

Switch Port Mode Interfaces for an FDM-Managed Device

For each physical Firepower 1010 interface, you can set its operation as a firewall interface or as a switch port. Switch ports forward traffic at Layer 2, using the switching function in hardware. Switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the FDM-managed device security policy. Access ports accept only untagged traffic, and you can assign them to a single VLAN. Trunk ports accept untagged and tagged traffic, and can belong to more than one VLAN. For devices that have been reimaged to Version 6.4, Ethernet 1/2 through 1/8 are configured as access switch ports on VLAN 1; devices that are manually upgraded to Version 6.4 (and later), the ethernet configuration maintains the configuration prior ot upgrading. Note that switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the FDM-managed device security policy.

Access or Trunk

A physical interface configured as a switch port can be assigned as either an access port or a trunk port.

Access ports forward traffic to only one VLAN and accept only untagged traffic. We strongly recommend this option if you intend to forward traffic to a single host or device. You must also specify the VLAN you would like to be associated with the interface, otherwise it will default to VLAN 1.

Trunk ports forward traffic to multiple VLANs. You must assign one VLAN interface as the native trunk port and at least one VLAN as an associated trunk port. You can select up to 20 interfaces to be associated with the switch port interface, which enables traffic from different VLAN IDs to pass through the switch port interface. If an untagged traffic is passed through the switch port then the traffic is tagged with the VLAN ID of the native VLAN interface. Note that the default Fiber Distributed Data Interface (FDDI) & Token RING ID between 1002 and 1005 cannot be used for VLAN ID.

Change the Port Mode

If you select an interface that is configured for routed mode as a VLAN member, Security Cloud Control automatically converts the interface to switch port mode and configures the interface as an access port by default. As a result the logical name and the associated static IP addresses are removed from the interface.

Configuration Limitations

Be aware of the following limitations:

- Only physical Firepower 1010 devices support switch port mode configuration. Virtual FDM-managed devices do not support switch port mode.
- The Firepower 1010 device allows a maximum of 60 VLANs.
- VLAN interfaces configured for switch port mode must be unnamed. This means the MTU **must** be configured to 1500 bytes.
- You **cannot** delete an interface configured as a switch port mode. You must manually change the interface mode from **switch port** mode to **routed** mode.
- Interfaces configured for switch port mode do not support IP addresses. If the interface is currently referenced in or configured for VPN, DHCP, or is associated with a static route, you **must** manually remove the IP address.
- You cannot use any member of the bridge group interface as a switch port.
- The MTU for a VLAN interface **must** be 1500 bytes. Unnamed VLAN interfaces do not support any other configuration.
- Switch port mode does not support the following:
    - Diagnostic interface.
    - Dynamic, multicast, or Equal-Cost Multi-Path (ECMP) routing.
    - Passive interfaces.
    - Port etherchannels, or using an interface that is a member of an etherchannel.
    - Subinterfaces.
    - Failover and state link.

High Availability and Switch Port Mode Interfaces

You should not use the switch port functionality when using High Availability. Because the switch ports operate in hardware, they continue to pass traffic on both the active *and* the standby units. High Availability is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal High Availability network setup, active switch ports on both units will lead to network

loops. We suggest that you use external switches for any switching capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot.

Note You can only use a firewall interface as the failover link.

Switch Port Mode Configurations in Templates

You can create templates of devices with interfaces configured for switch port mode. Beware the following scenarios when mapping interfaces from the template to a device:

- If a template interface does not contain any VLAN members prior to applying the template, Security Cloud Control automatically maps it to an available device interface that has the same properties.
- If a template interface that does not contain a VLAN member is mapped to a device interface that is configured as **N/A**, Security Cloud Control automatically creates an interface on the device the template is to be applied to
- If a template interface containing a VLAN member is mapped to a device interface that is not present, applying a template will **fail**.
- Templates do not support mapping more than one template interface to the same device interface.
- The template's management interface must be mapped to the device's management interface.

Configure an FDM-Managed Device VLAN

You must first configure a VLAN interface if you intend to configure subinterfaces or switch ports.

Note An FDM-managed device supports a maximum of 60 VLAN interfaces.

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the desired device you want to create a VLAN on.

Step 4 In the **Management** pane at the right, click **Interfaces**.

Step 5 On the **Interfaces** page, click the + button.

Step 6 Configure the following:

- **Parent Interface** - The parent interface is the physical interface to which you want to add the subinterface. You cannot change the parent interface after you create the subinterface.
- (Optional) **Logical Name**-Set the name for the VLAN, up to 48 characters. Alphabetic characters must be lower case. If you do not want to route between the VLAN and other VLANs or firewall interfaces, then leave the VLAN interface name empty.

Note If you do not enter a name, the MTU in the **Advanced Options** must be set to 1500. If you change the MTU to something other than 1500, the VLAN must be unnamed.

- (Optional) **Description**-The description can be up to 200 characters on a single line, without carriage returns.
- (Optional) **Security Zone** - Assign the subinterface to a security zone. Note that you cannot assign a subinterface if it does not have a Logical Name. You ca also assign a security zone after creating a subinterface. See Use of Security Zones in Firepower Interface Settings for more information.
- (Optional) **VLAN ID**-Enter the VLAN ID between 1 and 4070 that will be used to tag the packets on this subinterface.

  Note VLAN interfaces are routed by default. If you add this VLAN interface to a bridge group at a later date, Security Cloud Control automatically changes the mode to **BridgeGroupMember**. Similarly, if you change this VLAN interface to switch port mode, Security Cloud Control automatically changes the mode to **Switch Port**.

- (Optional) **Subinterface ID** - Enter the subinterface ID as an integer between 1 and 4294967295. This ID is appended to the interface ID; for example Ethernet1/1.100. You can match the VLAN ID for convenience, but it is not required. You cannot change the ID after you create the subinterface.

Step 7 Click the **IPv4 Address** tab and select one of the following options from the Type field:

- **Static** - Choose this option if you want to assign an address that should not change. Type in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address is not already used on the network.

  If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

  Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See Configure DHCP Servers for more information.

- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. You cannot use this option if you configure high availability. Change the following options if necessary:
  - **Route Metric**-If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
  - **Obtain Default Route**-Check this option to get the default route from the DHCP server. You would normally select this option, which is the default.

- **DHCP Address Pool** - If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes.

Step 8 (Optional) Click the **IPv6 Address** tab and configure the following:

- **State** - To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, slide the State slider to blue. The link local address is generated based on the interface MAC addresses (Modified EUI-64 format).

  Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Address Auto Configuration** - Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.
- **Suppress RA**-Whether to suppress router advertisements. Threat Defense can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately auto-configure without needing to wait for the next scheduled router advertisement message.

  We suggest suppressing these messages on any interface for which you do not want the FDM-managed device to supply the IPv6 prefix (for example, the outside interface).
- **Static Address/Prefix**-If you do not use stateless auto configuration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing for Firepower Interfaces.
- **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 9 (Optional) Click the **Advanced** tab.

- Select **Enable** for **HA Monitoring** if you want the health of the interface to be a factor when the system decides whether to fail over to the peer unit in a high availability configuration.

  This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
- Select **Management Only** to make a data interface management only.

  A management only interface does not allow through traffic, so there is very little value in setting a data interface as management only. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- Modify the IPv6 Configuration settings.
  - **Enable DHCP for IPv6 address configuration**-Whether to set the Managed Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.

- **Enable DHCP for IPv6 non-address configuration**-Whether to set the Other Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.
- **DAD Attempts**-How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless autoconfiguration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- Change the **MTU** (maximum transmission unit) to the desired value.

  The default MTU is 1500 bytes. You can specify a value from 64 - 9198 (or 9000 for virtual FDM-managed devices and 9184 for the Firepower 4100/9300). Set a high value if you typically see jumbo frames on your network.

  Note If you increase MTU above 1500 on ASA 5500-X series devices, ISA 3000 series devices, or virtual FDM-managed devices, the VLAN must be unnamed **and** you must reboot the device. Log into the CLI and use the reboot command. If the device is configured for HA, you must also reboot the standby device. You do not need to reboot Firepower models, where jumbo frame support is always enabled.

- (Optional for subinterface and HA pairs) Configure the **MAC address**.

  By default, the system uses the MAC address burned into the network interface card (NIC) for the interface. Thus, all subinterfaces on an interface use the same MAC address, so you might want to create unique addresses per subinterface. Manually configured active/standby MAC addresses are also recommended if you configure high availability. Defining the MAC addresses helps maintain consistency in the network in the event of failover.

  - **MAC Address**-The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
  - **Standby MAC Address**-For use with HA pairs. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 10 If you intend to create another subinterface for this device, check **Create another** prior to completing the subinterface configuration.

Step 11 (Optional) Activate the subinterface upon creation by toggling the **State** slider in the upper right corner of the pop-up window from grey to blue.

Step 12 Click **OK**.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure an FDM-Managed Device VLAN for Switch Port Mode

Be sure to read the limitations for switch port mode prior to configuration; see Switch Port Mode Interfaces for an FDM-Managed Device for more information.

Note You can assign or edit a VLAN member to a physical interface at any time. Be sure to deploy the changes to the device after you confirm the new configuration.

Create a VLAN Interface for Switch Port Mode

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to configure interfaces for.

Step 4 In the **Management** pane on the right, click **Interfaces**.

Step 5 On the **Interfaces** page, click the + button and choose **VLAN Interface**.

Step 6 View the **VLAN Members** tab and select the desired physical interfaces.

Note If you chose to add a member that references a VLAN interface configured for either Access or Native Trunk, you can only select one VLAN as a member. Physical interfaces that references a VLAN interface configured for Associated Trunk supports up to 20 interfaces as members.

Step 7 Configure the rest of the VLAN interface, as described in Configure an FDM-Managed Device VLAN.

Step 8 Click **Save**. Confirm that you want to reset the VLAN configuration and reassign an IP address to the interface.

Step 9 Preview and Deploy Configuration Changes for All Devicesnow the changes you made, or wait and deploy multiple changes at once.

Configure an Existing Physical Interface for Switch Port Mode

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to configure interfaces for.

Step 4 In the **Management** pane on the right, click **Interfaces**.

Step 5 On the **Interfaces** page, select the physical interface you want to modify. In the Action Pane on the right, click the edit icon .

Step 6 Interfaces configured for switch port mode do not support logical names. If the interface has a logical name, delete it.

Step 7 Locate the **Mode** and use the drop-down menu to select **Switch Port**.

Step 8 Configure the physical interface for switch port mode:

- (Optional) Check the **Protected Port** check box to set this switch port as protected, so you can prevent the switch port from communicating with other protected switch ports on the same VLAN. You might want to prevent switch ports from communicating with each other if: the devices on those switch ports are primarily accessed from other VLANs; you do not need to allow intra-VLAN access; and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply this option to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
- For the Usage Type, select **Access** or **Trunk**. See Switch Port Mode Interfaces for an FDM-Managed Device to determine which port type you need.
  - If you select **Trunk**, you must select one VLAN interface as the **Native Trunk VLAN** to forward untagged traffic and at least one **Associated VLAN** to forward tagged traffic. Click the  icon to view the existing physical interfaces. You can select up to 20 VLAN interfaces as associated VLANs.
  - You can create a new VLAN interface set to Access mode by clicking **C reate new VLAN**.

Step 9 Click **Save**. Confirm that you want to reset the VLAN configuration and reassign an IP address to the interface.

Step 10 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Viewing and Monitoring Firepower Interfaces

To view firepower interfaces, follow these steps:

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and the device whose interfaces you want to view.

Step 4 Select **Interfaces** in the Management pane on the right.

Step 5 In the Interfaces table, select an interface.

- If you expand the interface row, you see subinterface information.
- On the right, you see detailed interface information.

Monitoring Interfaces in the CLI

You can view some basic information, behavior, and statistics about interfaces by connecting to the device using SSH and running the command below.

For an easy to connect to the device using SSH, onboard the FDM-managed device you want to monitor as an SSH device and then use the >_ Command Line Interface in Security Cloud Control.

- **`show interface`** displays interface statistics and configuration information. This command has many keywords you can use to get to the information you need. Use ? as a keyword to see the available options.
- **`show ipv6 interface`** displays IPv6 configuration information about the interfaces.
- **`show bridge-group`** displays information about Bridge Virtual Interfaces (BVI), including member information and IP addresses.
- **`show conn`** displays information about the connections currently established through the interfaces.
- **`show traffic`** displays statistics about traffic flowing through each interface.
- **`show ipv6 traffic`** displays statistics about IPv6 traffic flowing through the device.
- **`show dhcpd`** displays statistics and other information about DHCP usage on the interfaces, particularly about the DHCP servers configured on interfaces.

Synchronizing Interfaces Added to a Firepower Device using FXOS

If an interface is added to a Firepower device by using the Firepower eXtensible Operating System (FXOS) Chassis Manager, on the Firepower 4100 series or 9300 series devices, Security Cloud Control does *not* recognize that configuration change and report a configuration conflict.

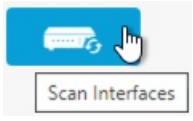
To see the newly added interface in Security Cloud Control, follow this procedure:

Procedure

Step 1 Log in to an FDM-managed device.

Step 2 From the FDM-managed main page, click **View All Interfaces** in the Interfaces panel.

Step 3 Click the **Scan Interfaces** button:



Step 4 Wait for the interfaces to scan, and then click **OK**.

Step 5 Deploy your changes on an FDM-managed device.

Step 6 Log in to Security Cloud Control as an Admin or SuperAdmin.

Step 7 In the navigation pane, click **Inventory**.

Step 8 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 9 Click the **FTD** tab and select the device with the expected new interface configuration.

Step 10 Click **Check for Changes** to immediately compare the copy of the configuration on the device with the copy of the configuration stored on Security Cloud Control. Security Cloud Control will detect the interface change and report a "Conflict Detected" state on the **Inventory** page for the device.

Step 11 Resolve the Conflict Detected by clicking **Review Conflict** and then accepting the out of band changes.

Routing

Routing is the act of moving information across a network from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing involves two basic activities: determining optimal routing paths and transporting packets through a network.

Using Security Cloud Control, you can define a default route, and other static routes, for your FDM-managed devices. The following topics explain routing basics and how to use Security Cloud Control to configure static routing on your FDM-managed device:

- About Static Routing and Default Routes
- The Routing Table and Route Selection
- Configure Static and Default Routes for FDM-Managed Devices
- Monitoring Routing

About Static Routing and Default Routes

To route traffic to a non-connected host or network, you must define a route to that host or network. That defined route is a static route. Consider also configuring a default route. A default route is for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

Related Information:

- Default Route
- Static Routes

Default Route

If you do not know a route to a specific network, the simplest option is to configure a default route that sends all traffic to an upstream router, relying on that router to route the traffic for you. A default route identifies the gateway IP address to which the FDM-managed device sends all IP packets for which you did not define a static route. A default route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

Static Routes

A static route is a route from one network to another network that you define and enter manually into the routing table. You might want to use static routes in the following cases:

- Your network is small and stable and you can easily manage manually adding and changing routes between devices.
- Your networks use an unsupported router discovery protocol.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the FDM-managed device.
- You are using a feature that does not support dynamic routing protocols.

Limitations:

- Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores the VTI interfaces. If a security zone or static route references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference. Security Cloud Control support for VTI tunnels is coming soon.
- FDM-managed device running on software version 7.0 or later allows configuring Equal-Cost Multi-Path (ECMP) traffic zones. When the FDM-managed device is onboarded to Security Cloud Control, it can read but cannot modify the ECMP configuration available in the global VRF routes because it does not allow a route to the same destination network with an identical metric value. You can create and modify ECMP traffic zones through FDM and then read it into Security Cloud Control. For more information on ECMP, see the "Equal-Cost Multi-Path (ECMP) Routing" section in the "Routing Basics and Static Routes" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0 or later.

The Routing Table and Route Selection

When NAT translations (xlates) and rules do not determine the egress interface, the system uses the routing table to determine the path for a packet.

Routes in the routing table include a metric called "administrative distance" that provides a relative priority to a given route. If a packet matches more than one route entry, the one with the lowest distance is used. Directly connected networks (those defined on an interface) have the distance 0, so they are always preferred. Static routes have a default distance of 1, but you can create them with any distance between 1-254.

Routes that identify a specific destination take precedence over the default route (the route whose destination is 0.0.0.0/0 or ::/0).

How the Routing Table is Populated

The FDM-managed device routing table can be populated with statically defined routes and directly connected routes. It is possible that the same route is entered in more than one manner. When two routes to the same destination are put into the routing table, the one that remains in the routing table is determined as follows:

- If the two routes have different network prefix lengths (network masks), then both routes are considered unique and are entered into the routing table. The packet forwarding logic then determines which of the two to use.

For example, assume the following routes are entered in the routing table:

- 192.168.32.0/24
- 192.168.32.0/19

Even though the 192.168.32.0/24 route has the longer network prefix, both routes are installed in the routing table because each of these routes has a different prefix length (subnet mask). They are considered different destinations and the packet forwarding logic determines which route to use.

- If multiple paths to the same destination are entered in the routing table, the route with the better metric, as entered with the static route, is entered into the routing table.

Metrics are values associated with specific routes, ranking them from most preferred to least preferred. The parameters used to determine the metrics differ for different routing protocols. The path with the lowest metric is selected as the optimal path and installed in the routing table. If there are multiple paths to the same destination with equal metrics, load balancing is done on these equal cost paths.

Related Information:

- How Forwarding Decisions are Made

How Forwarding Decisions are Made

Forwarding decisions are made in this order:

- Use NAT translations (xlates) and rules to determine the egress interface. If the NAT rules do not determine the egress interface, the system uses the routing table to determine the path for a packet.
- If the destination does not match an entry in the routing table, the packet is forwarded through the interface specified for the default route. If a default route has not been configured, the packet is discarded.
- If the destination matches a single entry in the routing table, the packet is forwarded through the interface associated with that route.
- If the destination matches more than one entry in the routing table, then the packet is forwarded out of the interface associated with the route that has the longer network prefix length. For example, a packet destined for 192.168.32.1 arrives on an interface with the following routes in the routing table:
- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

In this case, a packet destined to 192.168.32.1 is directed toward 10.1.1.2, because 192.168.32.1 falls within the 192.168.32.0/24 network. It also falls within the other route in the routing table, but 192.168.32.0/24 has the longer prefix within the routing table (24 bits verses 19 bits). Longer prefixes are always preferred over shorter ones when forwarding a packet.

Note Existing connections continue to use their established interfaces even if a new similar connection would result in different behavior due to a change in routes.

Configure Static and Default Routes for FDM-Managed Devices

Define static routes on an FDM-managed device so it knows where to send packets bound for networks not directly connected to the interfaces on the system.

Consider creating a default route. This is the route for network 0.0.0.0/0. This route defines where to send packets whose egress interface cannot be determined by existing NAT translations, static NAT rules, or other static routes.

You might need other static routes if the default gateway cannot be used to get to all networks. For example, the default route is usually an upstream router on the outside interface. If there are additional inside networks that are not directly connected to the device, and they cannot be accessed through the default gateway, you need static routes for each of those inside networks.

You cannot define static routes for the networks that are directly connected to system interfaces. The system automatically creates these routes.

Procedure

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** device and select the device on which you want to define static routes.

Step 4 In the **Management** pane at the right, click **Routing**.

Step 5 On the Static Routing page, do one of the following:

- To add a new static route, click the plus button  .
- Click the edit icon for the route you want to edit.

If you no longer need a route, click the trash can icon for the route to delete it.

Step 6 Configure the route properties

- **Protocol**-Select whether the route is for an IPv4 or IPv6 address.
- **Interface**-Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.
- **Gateway**-Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.
- **Metric**-The administrative distance for the route, between 1 and 254. The default is for static routes is 1. If there are additional routers between the interface and the gateway, enter the number of hops as the administrative distance.

  Administrative distance is a parameter used to compare routes. The lower the number, the higher precedence the route is given. Connected routes (networks directly connected to an interface on the device) always take precedence over static routes.

- **Destination Network**-Select the network object(s), that identifies the destination network, that contains the host(s), that uses the gateway in this route.

  To define a default route, use the pre-defined any-ipv4 or any-ipv6 network objects, or create an object for the 0.0.0.0/0 (IPv4) or ::/0 (IPv6) network.

Step 7 Click **OK**.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Static Route Example

See the Static Route Network Diagram for the addresses used in this example.

The goal is to create a static route that allows return traffic to the host at 20.30.1.2 in destination network 20.30.1.0/24.

The packet can take any path to reach the destination. When a network receives a packet on an interface, it determines where to forward the packet for the best route to a destination.

Note The DMZ does not have a static route as it is connected directly to the interface.

For example, consider the following two routes for reaching the destination.

Route 1:

Procedure

Step 1 Packets come back to the outside interface, **209.165.201.0/27**, looking for **20.30.1.2.**

Step 2 We direct the packets to use the **inside** interface to get to the gateway 192.168.1.2, which is on the same network as the destination.

Step 3 From there, we identify the destination network by the **gateway address** for that network, 20.30.1.1.

Step 4 The IP address 20.30.1.2 is on the same subnet as 20.30.1.1. The router forwards the packet to the switch, the switch forwards the packet to 20.30.1.2.

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.1.2 Metric: 1

Route 2:

Procedure

Step 1 Packets come back to the outside interface, **209.165.201.0/27**, looking for **20.30.1.2**.

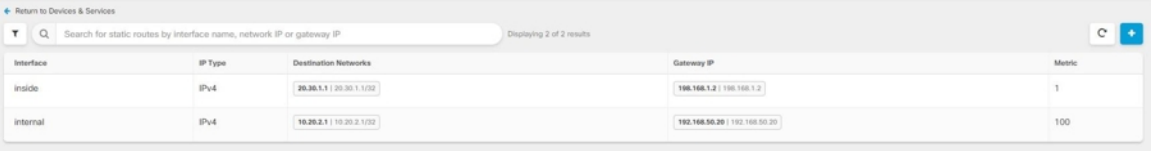
Step 2 We direct the packets to use the **internal** interface to get to the gateway 192.168.50.20, which is multiple hops away from the destination network.

Step 3 From there, we identify the destination network by the **gateway address** for that network, 20.30.1.1.

Step 4 The IP address 20.30.1.2 is on the same subnet as 20.30.1.0. The router forwards the packet to the switch, the switch forwards the packet to 20.30.1.2.

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.50.20 Metric: 100

Here is what the completed Add Static Route table would like for these routes.



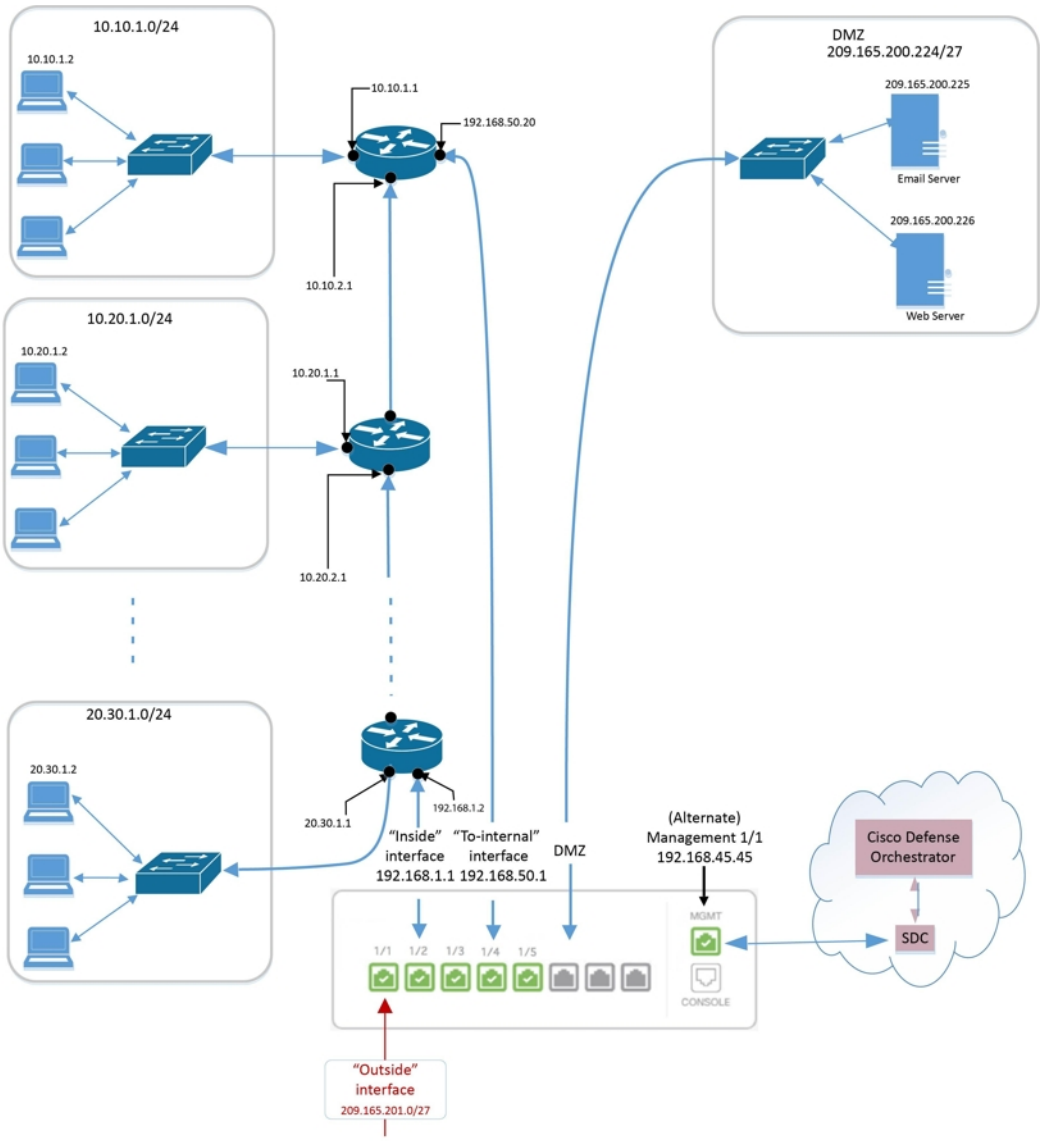
Monitoring Routing

To monitor and troubleshoot routing, open Firewall Device Manager for the device and open the CLI console or log into the device CLI using SSH and use the following commands:

- `show route` displays the routing table for the data interfaces, including routes for directly-connected networks.
- `show ipv6 route` displays the IPv6 routing table for the data interfaces, including routes for directly-connected networks.
- `show network` displays the configuration for the virtual management interface, including the management gateway. Routing through the virtual interface is not handled by the data interface routing table, unless you specify data-interfaces as the management gateway.
- `show network-static-routes` displays static routes configured for the virtual management interface using the `configure network static-routes` command. Normally, there will not be any static routes, as the management gateway suffices for management routing in most cases. These routes are not available to traffic on the data interfaces. This command is not available in the CLI console.

Static Route Network Diagram

We refer to this network diagram when discussing Configure Static and Default Routes for FDM-Managed Devices:



About Virtual Routing and Forwarding

About VRF

Virtual routing and forwarding (VRF) allow multiple instances of a routing table to exist in a router. Firepower Version 6.6 introduces the ability to have a default VRF table and user-created VRF tables. A single VRF table can handle multiple types of varying routing protocols, such as EX, OSPF, BGP, IGRP, etc. Each routing protocol within a VRF table is listed as an entry. In addition to handling multiple types of common routing protocols, you can configure a routing protocol to reference an interface from another VRF. This allows you to segment network paths without using multiple devices.

See About Virtual Routers and Virtual Routing and Forwarding (VRF) for more information.

VRF in Security Cloud Control

This feature is new to Firepower Version 6.6. When the FDM-managed device is onboarded to Security Cloud Control, the device routing page reads and supports only the VRFs defined on the global router of the FDM-managed device. To view the global VRF in Security Cloud Control, select the device from the **Inventory** page and select **Routing** from the **Management** pane located to the right of the window. From here, you can view, modify, and delete the global VRF; note that Security Cloud Control retains the name of the VRF when reading the configuration from FDM.

Security Cloud Control firewall device manager doesn't read VRFs configured in the user-defined virtual routers. You must create and manage VRF tables through firewall device manager.

For information on global and user-defined routes, see the "Managing Virtual Routers" section in the "Virtual Routers" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0 or later.

Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, Security Cloud Control recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

Security Cloud Control calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon:
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy. Before 28 June 2024, when you use an unassociated object in a rule or policy, Security Cloud Control created a copy of it and used the copy. Because of this behavior, you might have observed that there were two instances of the same object in the **Objects** menu. However, Security Cloud Control does not do that anymore. You can use an unassociated object in a rule or a policy but there are no duplicate objects that Security Cloud Control creates.

You can view the objects managed by Security Cloud Control by navigating to the **Objects** menu or by viewing them in the details of a network policy.

Security Cloud Control allows you to manage network and service objects across supported devices from one location. With Security Cloud Control, you can manage objects in these ways:

- Search for and Object Filters based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects in use by a device after it has been on-boarded to Security Cloud Control.

Note Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes on devices, see Out-of-Band Changes on Devices, on page 575.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Security Cloud Control, on page 744 for more information.

Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, Security Cloud Control recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

Security Cloud Control calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon:
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy. Before 28 June 2024, when you use an unassociated object in a rule or policy, Security Cloud Control created a copy of it and used the copy. Because of this behavior, you might have observed that there were two instances of the same object in the **Objects** menu. However, Security Cloud Control does not do that anymore. You can use an unassociated object in a rule or a policy but there are no duplicate objects that Security Cloud Control creates.

You can view the objects managed by Security Cloud Control by navigating to the **Objects** menu or by viewing them in the details of a network policy.

Security Cloud Control allows you to manage network and service objects across supported devices from one location. With Security Cloud Control, you can manage objects in these ways:

- Search for and Object Filters based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects in use by a device after it has been on-boarded to Security Cloud Control.

Note Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes on devices, see Out-of-Band Changes on Devices, on page 575.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Security Cloud Control, on page 744 for more information.

Object Types

The following table describes the objects that you can create for your devices and manage using Security Cloud Control.

Table 10: Common Objects

Object Type	Description
Network	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
URL	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

Table 11: FDM-Managed Device Object Types

Object	Description
Application Filter Objects	An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.
Upload RA VPN AnyConnect Client Profile	AnyConnect Client Profile objects are file objects and represent files used in configurations, typically for remote access VPN policies. They can contain an AnyConnect Client Profile and AnyConnect Client Image files.
Certificate Objects	Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.
DNS Group Objects	DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.
Create and Edit a Firepower Geolocation Filter Object	A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses.
Create or Edit an IKEv1 Policy	An IKEv1 policy object contain the parameters required for IKEv1 policies when defining VPN connections.
IKEv2 Policy	An IKEv2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections.
IKEv1 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 1 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
IKEv2 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
Network Objects	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.

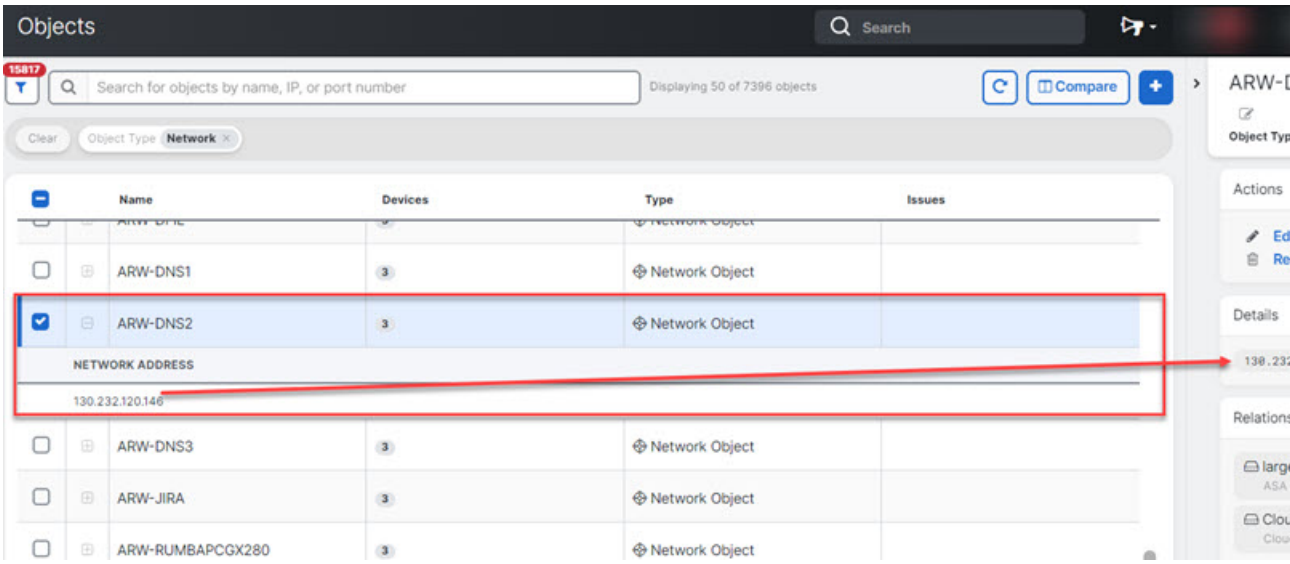
Object	Description
Security Zone Object	A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic.
Service Objects	Service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the TCP/IP protocol suite.
Create an SGT Group	A SGT dynamic object identifies source or destination addresses based on an SGT assigned by ISE and can then be matched against incoming traffic.
Syslog Server Objects	A syslog server object identifies a server that can receive connection-oriented or diagnostic system log (syslog) messages.
URL Objects	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

Shared Objects

Security Cloud Control calls objects on multiple devices with the same name and same contents, **shared objects**. Shared objects are identified by this icon

on the **Objects** page. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

When looking at a shared object, Security Cloud Control shows you the contents of the object in the object table. Shared objects have exactly the same contents. Security Cloud Control shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.



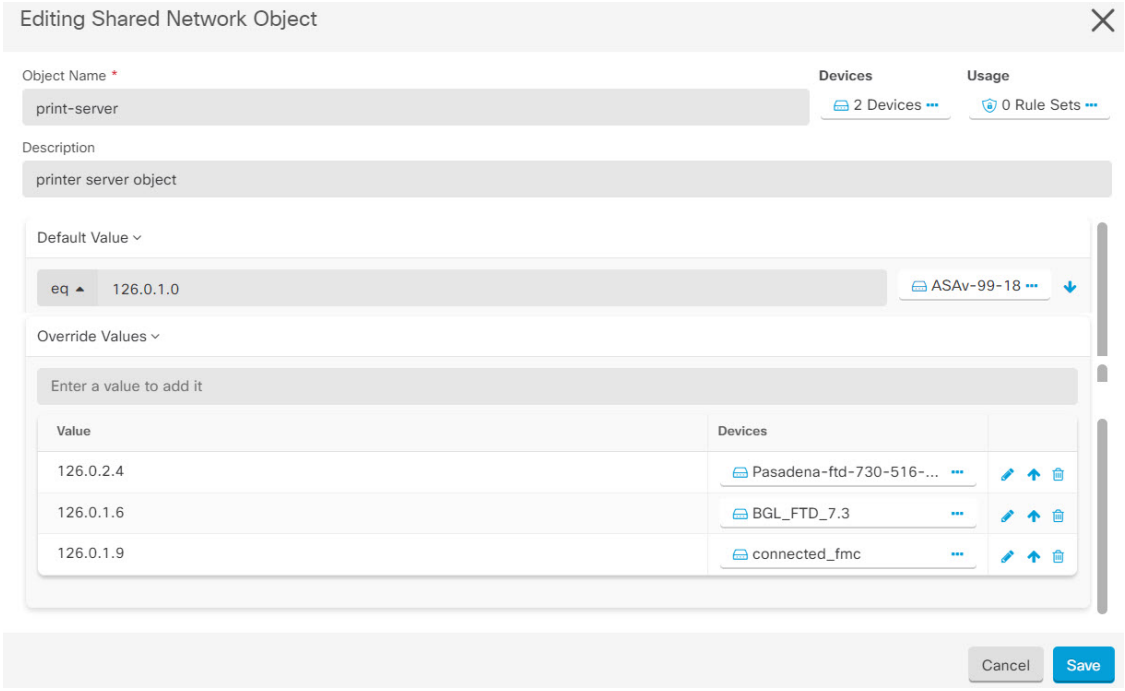
Object Overrides

An object override allows you to override the value of a shared network object on specific devices. Security Cloud Control uses the corresponding value for the devices that you specify when configuring the override. Although the objects are on two or more devices with the same name but different values, Security Cloud Control doesn't identify them as **Inconsistent objects** only because these values are added as overrides.

You can create an object whose definition works for most devices, and then use overrides to specify modifications to the object for the few devices that need different definitions. You can also create an object that needs to be overridden for all devices, but its use allows you to create a single policy for all devices. Object overrides allow you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices.

For example, consider a scenario where you have a printer server in each of your offices, and you have created a printer server object `print-server`. You have a rule in your ACL to deny printer servers from accessing the internet. The printer server object has a default value that you want to change from one office to another. You can do this by using object overrides and maintain rule and "printer-server" object consistent across all locations, although their values may be different.

Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes, see Out-of-Band Changes on Devices, on page 575.



Note Security Cloud Control allows you to override objects associated with the rules in a ruleset. When you add a new object to a rule, you can override it only after you attach a device to the ruleset and save the changes. See Configure Rulesets for a Device for more information.

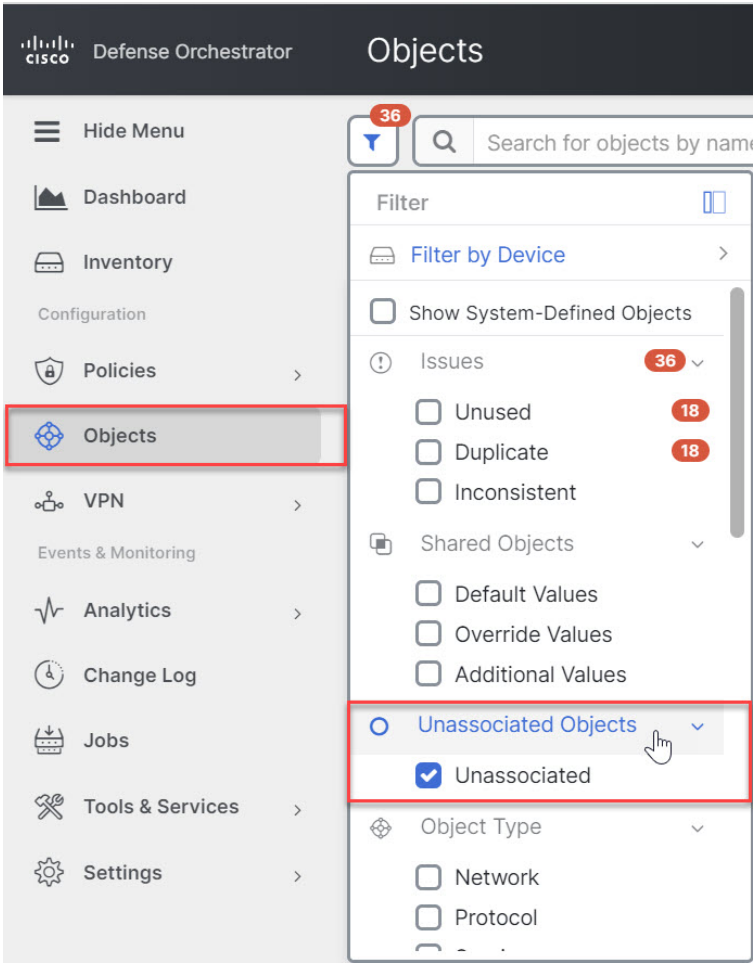
Note If there are inconsistent objects, you can combine them into a single shared object with overrides. For more information, see Resolve Inconsistent Object Issues, on page 751.

Unassociated Objects

You can create objects for immediate use in rules or policies. You can also create an object that is unassociated with any rule or policy. When you use that unassociated object in a rule or policy, Security Cloud Control creates a copy of it and uses the copy. The original unassociated object remains among the list of available objects until it is either deleted by a nightly maintenance job, or you delete it.

Unassociated objects remain in Security Cloud Control as a copy to ensure that not all configurations are lost if the rule or policy associated with the object is deleted accidentally.

To view unassociated objects click in the left-hand pane of the Objects tab and check the **Unassociated** checkbox.

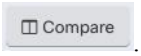


Compare Objects

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Filter the objects on the page to find the objects you want to compare.

Step 3 Click the **Compare** button 

.

Step 4 Select up to three objects to compare.

Step 5 View the objects, side-by-side, at the bottom of the screen.

- Click the up and down arrows in the Object Details title bar to see more or less of the Object Details.
- Expand or collapse the Details and Relationships boxes to see more or less information.

Step 6 (Optional) The Relationships box shows how an object is used. It may be associated with a device or a policy. If the object is associated with a device, you can click the device name and then click **View Configuration**

to see the configuration of the device. Security Cloud Control shows you the device's configuration file and highlights the entry for that object.

Filters

You can use many different filters on the **Inventory** and **Objects** pages to find the devices and objects you are looking for.

To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

Note When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.

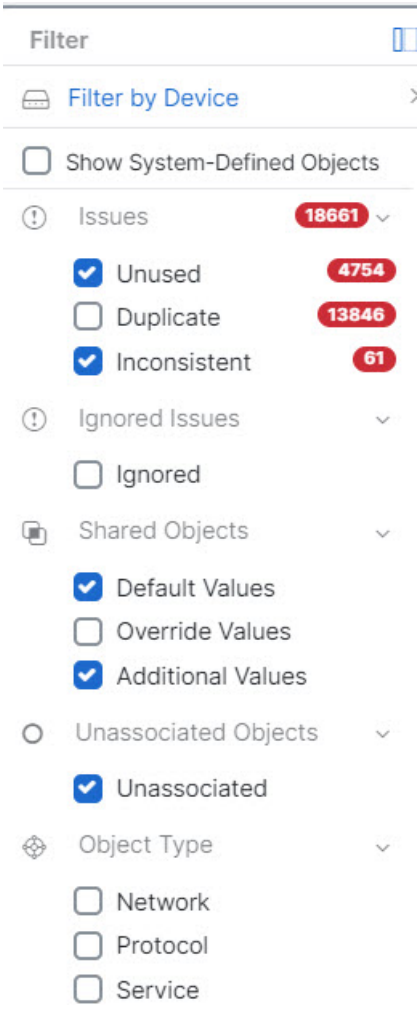
- FDM: Devices managed using FTD API or FDM.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

The object type filter allows you to filter objects by type, such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter allows filtering objects having default values or override values.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values.



Object Filters

To filter, click in the left-hand pane of the Objects tab:

- **Filter by Device**: Lets you pick a specific device so that you can see objects found on the selected device.
- **Issues**: Lets you pick unused, duplicate, and inconsistent objects to view.
- **Ignored Issues**: Lets you view all the objects whose inconsistencies you had ignored.
- **Shared Objects**: Lets you view all the objects that Security Cloud Control has found to be shared on more than one device. You can choose to see shared objects with only default values or override values, or both.
- **Unassociated Objects**: Lets you view all the objects that are not associated with any rule or policy.
- **Object Type**: Lets you select an object type to see only those type of objects that you have selected, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

Sub filters – Within each main filter, there are sub-filters you can apply to further narrow down your selection. These sub-filters are based on Object Type – Network, Service, Protocol, etc.

The selected filters in this filter bar would return objects that match the following criteria:

***** Objects that are on one of two devices. (Click **Filter by Device** to specify the devices.) AND are

*** Inconsistent** objects AND are

*** Network** objects OR **Service** objects AND

***** Have the word "**group**" in their object naming convention

Because **Show System Objects** is checked, the result would include both system objects and user-defined objects.

Show System-Defined Objects Filter

Some devices come with pre-defined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

Show System-Defined Objects is **off** by default. To display system objects in the object table, check **Show System-Defined Objects** in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

If you hide system objects, they will not be included in your search and filtering results. If you show system objects, they will be included in your object search and filtering results.

Configure Object Filters

You can filter on as few or as many criteria as you want. The more categories you filter by, the fewer results you should expect.

Procedure

Step 1 In the left pane, click **Objects**.

Step 2 Open the filter panel by clicking the filter icon at the top of the page. Uncheck any filters that have been checked to make sure no objects are inadvertently filtered out. Additionally, look at the search field and delete any text that may have been entered in the search field.

Step 3 If you want to restrict your results to those found on particular devices:

a. Click **Filter By Device**.

b. Search all the devices or click a device tab to search for only devices of a certain kind.

c. Check the device you want to include in your filter criteria.

d. Click **OK**.

Step 4 Check **Show System Objects** to include system objects in your search results. Uncheck **Show System Objects** to exclude system objects from your search results.

Step 5 Check the object **Issues** you want to filter by. If you check more than one issue, objects in any of the categories you check are included in your filter results.

Step 6 Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.

Step 7 Check the required filter in **Shared Objects** if you are filtering for objects shared between two or more devices.

- **Default Values**: Filters objects having only the default values.
- **Override Values**: Filters objects having overridden values.
- **Additional Values**: Filters objects having additional values.

Step 8 Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.

Step 9 Check the **Object Types** you want to filter by.

Step 10 You can also add an object name, IP address, or port number to the Objects search field to find objects with your search criteria among the filtered results.

When to Exclude a Device from Filter Criteria

When adding a device to filtering criteria, the results show you the objects on a device but not the relationships of those objects to other devices. For example, assume **ObjectA** is shared between ASA1 and ASA2. If you were to filter objects to find shared objects on ASA1, you would find **ObjectA** but the **Relationships** pane would only show you that the object is on ASA1.

To see all the devices to which an object is related, don't specify a device in your search criteria. Filter by the other criteria and add search criteria if you choose to. Select an object that Security Cloud Control identifies and then look in the Relationships pane. You will see all the devices and policies the object is related to.

Unignore Objects

One way to resolve unused, duplicate, or inconsistent objects is to ignore them. You may decide that though an object is Resolve an Unused Object Issue, a Resolve Duplicate Object Issues, or Resolve Inconsistent Object Issues, there are valid reasons for that state and you choose to leave the object issue unresolved. At some point in the future, you may want to resolve those ignored objects. As Security Cloud Control does not display ignored objects when you search for object issues, you will need to filter the object list for ignored objects and then act on the results.

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Object Filters.

Step 3 In the **Object** table, select the object you want to unignore. You can unignore one object at a time.

Step 4 Click **Unignore** in the details pane.

Step 5 Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

Deleting Objects

You can delete a single object or mulitple objects.

Delete a Single Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects**.

Step 2 Locate the object you want to delete by using object filters and the search field, and select it.

Step 3 Review the **Relationships** pane. If the object is used in a policy or in an object group, you cannot delete the object until you remove it from that policy or group.

Step 4 In the Actions pane, click the **Remove** icon .

Step 5 Confirm that you want to delete the object by clicking **OK**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Delete a Group of Unused Objects

As you onboard devices and start resolving object issues, you find many unused objects. You can delete up to 50 unused objects at a time.

Procedure

Step 1 Use the **Issues** filter to find **unused** objects. You can also use the Device filter to find objects that are not associated with a device by selecting **No Device**. Once you have filtered the object list, the object checkboxes appear.

Step 2 Check the **Select all** checkbox in the object table header to select all the objects found by the filter that appear in the object table; or, check individual checkboxes for individual objects you want to delete.

Step 3 In the Actions pane, click the **Remove** icon .

Step 4 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Network Objects

A network object can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. **Network groups** are collections of network objects and other individual addresses or subnetworks you add to the group. Network objects and network groups are used in access rules, network policies, and NAT rules. You can create, update, and delete network objects and network groups using Security Cloud Control.

Note that not all platforms support network objects, such as Cisco Merkai and Multicloud Defense; when you share dynamic objects, Security Cloud Control automatically translates the appropriate information from the originating platform or device into a set of usable information that Security Cloud Control can use.

Table 12: Pemitted Values of Network Objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Fully Qualified Domain Name	Subnet using CIDR Notation
FTD	IPv4 and IPv6	Yes	Yes	Yes	Yes
Multicloud Defense	IPv4 and IPv6	Yes	Yes	Yes	Yes

Table 13: Pemitted Contents of a Network Group

Device type	IP Value	Network Object	Network Groups
FTD	No	Yes	Yes
Multicloud Defense	Yes	Yes	Yes

Reusing Network Objects Across Products

If you have a Security Cloud Control tenant with a cloud-delivered Firewall Management Center and one or more on-premises management centers onboarded to your tenant:

- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object or group, a copy of the object is also added to the objects list on the **Objects > Other FTD Objects** page used when configuring cloud-delivered Firewall Management Center, and vice versa.
- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, or ASA network object or group, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the on-premises management center on which you want to use the object and discard the ones that you do not want. Navigate , **Administration** > **Firewall Management Center** select the on-premises management center, and click **Objects** to see your objects in the On-Premises Firewall Management Center user interface and assign them to policies.

Changes you make to network objects or groups on either page apply to the object or group instance on both pages. Deleting an object from one page also deletes the corresponding copy of the object from the other page.

Exceptions:

- If a network object of the same name already exists for cloud-delivered Firewall Management Center, the new Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object will not be replicated on the **Objects > Other FTD Objects** page of Security Cloud Control.
- Network objects and groups in onboarded threat defense devices that are managed by on-premises Secure Firewall Management Center are not replicated on the **Objects > Other FTD Objects** page and cannot be used in cloud-delivered Firewall Management Center.

  Note that for on-premises Secure Firewall Management Center instances that have been *migrated* to cloud-delivered Firewall Management Center, network objects and groups *are* replicated to the Security Cloud Control objects page if they are used in policies that were deployed to FTD devices.
- Sharing Network Objects between Security Cloud Control and cloud-delivered Firewall Management Center is automatically enabled on new tenants but must be requested for existing tenants. If your network objects are not being shared with cloud-delivered Firewall Management Center, How Security Cloud Control Customers Open a Support Ticket with TAC to have the features enabled on your tenant.
- Sharing network objects between Security Cloud Control and On-Premises Management Center is not automatically enabled on Security Cloud Control for new on-premises management centers onboarded to Security Cloud Control. If your network objects are not being shared with On-Premises Management Center, ensure **Discover & Manage Network Objects** toggle button is enabled for the on-premises management center in **Settings** or How Security Cloud Control Customers Open a Support Ticket with TAC to have the features enabled on your tenant.

Viewing Network Objects

Network objects you create using Security Cloud Control and those Security Cloud Control recognizes in an onboarded device's configuration are displayed on the Objects page. They are labeled with their object type. This allows you to filter by object type to quickly find the object you are looking for.

When you select a network object on the Objects page, you see the object's values in the Details pane. The Relationships pane shows you if the object is used in a policy and on what device the object is stored.

When you click on a network group you see the contents of that group. The network group is a conglomerate of all the values given to it by the network objects.

Related Information:

- Create or Edit a Firepower Network Object or Network Groups

Create or Edit a Firepower Network Object or Network Groups

A Firepower network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects and network groups that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

Firepower network objects and groups can be used by ASA, threat defense, FDM-managed, and Meraki devices. See Reusing Network Objects Across Products, on page 118.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Table 14: IP addresses that can be added to network objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Partially Qualified Domain Name (PQDN)	Subnet using CIDR Notation
Firepower	IPv4 / IPv6	Yes	Yes	Yes	Yes

Related Information:

- Create a Firepower Network Object, on page 120
- Edit a Firepower Network Object, on page 122
- Add Additional Values to a Shared Network Group, on page 125
- Edit Additional Values in a Shared Network Group, on page 127

Create a Firepower Network Object

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network object**.

Step 6 In the **Value** section:

- Select **eq** and enter a single IP address, a subnet address expressed in CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and enter an IP address range.

Note Do not set a host bit value. If you enter a host bit value other than 0, Security Cloud Control unsets it while creating the object, because the cloud-delivered Firewall Management Center only accepts IPv6 objects with host bits not set.

Step 7 Click **Add**.

Attention: The newly created network objects aren't associated with any FDM-managed device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters. For more information, see Configure Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create a Firepower Network Group

A **network group** can contain network objects and network groups. When you create a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects** > **FDM Objects** page, a copy of the object is automatically added to the **Objects** > **Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network group**.

Step 6 In the **Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.

Step 7 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 8 If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 9 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Note: You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.

Step 10 After adding the required objects, click **Save** to create a new network group.

Step 11 Preview and Deploy Configuration Changes for All Devices.

Edit a Firepower Network Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects** > **FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects** > **Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the network object and click the edit icon  in the **Actions** pane.

Step 4 Edit the values in the dialog box in the same fashion that you created them in "Create a Firepower Network Group".

Note Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit a Firepower Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the network group you want to edit by using object filters and search field.

Step 3 Select the network group and click the edit icon in the **Actions** pane.

Step 4 Change the object name and description if needed.

Step 5 If you want to change the objects or network groups that are already added to the network group, perform the following steps:

a. Click the edit icon appearing beside the object name or network group to modify them.

b. Click the checkmark to save your changes. **Note**: You can click the remove icon to delete the value from a network group.

Step 6 If you want to add new network objects or network groups to this network group, you have to perform the following steps:

a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, Security Cloud Control provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

b. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

c. If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.

- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 7 Click **Save**. Security Cloud Control displays the policies that will be affected by the change.

Step 8 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 9 Preview and Deploy Configuration Changes for All Devices.

Add an Object Override

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object to which you want to add an override, using object filters and search field.

Step 3 Select the network object and click the edit icon  in the **Actions** pane.

Step 4 Enter the value in the **Override Values** dialog box and click **+ Add Value**.

Important The override you are adding must have the same type of value that the object contains. For example, to a network object, you can configure an override only with a network value and not a host value.

Step 5 Once you see that the value is added, click the cell in the **Devices** column in **Override Values**.

Step 6 Click **Add Devices**, and choose the device to which you want the override to be added. The device you select must contain the object to which you are adding the override.

Step 7 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 8 Click **Confirm** to finalize the addition of the override to the object and any devices affected by it.

Note You can add more than one override to an object. However, you must select a different device, which contains the object, each time you are adding an override.

Step 9 See Object Overrides, on page 110 to know more about object overrides and Edit Object Overrides , on page 125 to edit an existing override.

Edit Object Overrides

You can modify the value of an existing override as long as the object is present on the device.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object having override you want to edit by using object filters and search field.

Step 3 Select the object having override and click the edit icon in the Actions pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click on the cell in the **Devices** column in **Override Values** to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Override Values** to push and make it as the default value of the shared object.
- Click the delete icon next to the override you want to remove.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Add Additional Values to a Shared Network Group

The values in a shared network group that are present on all devices associated with it are called "default values". Security Cloud Control allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When Security Cloud Control deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory". These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

Note If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See Resolve Inconsistent Object Issues, on page 751 for more information.

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the shared network group you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

- The **Devices** field shows the devices the shared network group is present.
- The **Usage** field shows the rulesets associated with the shared network group.
- The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.

Step 4 In the **Additional Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.

Step 5 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 6 If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 7 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 8 In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.

Step 9 Select the devices that you want and click **OK**.

Step 10 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 11 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 12 Preview and Deploy Configuration Changes for All Devices.

Edit Additional Values in a Shared Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the object having the override you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
- Click arrow in **Override Values** to push and make it as default objects of the shared network group.
- Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the or **Objects > FDM Objects** page deletes the replicated network object or group from the **Objects > Other FTD Objects** page and vice-versa.

URL Objects

URL objects and URL groups are used by Firepower devices. Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies. A URL object defines a single URL or IP address, whereas a URL group defines more than one URL or IP address.

Before You Begin

When creating URL objects, keep the following points in mind:

- If you do not include a path (that is, there is no / character in the URL), the match is based on the server's hostname only. The hostname is considered a match if it comes after the :// separator, or after any dot in the hostname. For example, ign.com matches ign.com and www.ign.com, but it does not match verisign.com.
- If you include one or more / character, the entire URL string is used for a substring match, including the server name, path, and any query parameters. However, we recommend that you do not use manual URL filtering to block or allow individual web pages or parts of sites, as servers can be reorganized and pages moved to new paths. Substring matching can also lead to unexpected matches, where the string you include in the URL object also matches paths on unintended servers or strings within query parameters.
- The system disregards the encryption protocol (HTTP vs HTTPS). In other words, if you block a website, both HTTP and HTTPS traffic to that website is blocked, unless you use an application condition to target a specific protocol. When creating a URL object, you do not need to specify the protocol when creating an object. For example, use example.com rather than http://example.com.
- If you plan to use a URL object to match HTTPS traffic in an access control rule, create the object using the subject common name in the public key certificate used to encrypt the traffic. Also, the system disregards subdomains within the subject common name, so do not include subdomain information. For example, use example.com rather than www.example.com.

  However, please understand that the subject common name in the certificate might be completely unrelated to a web site's domain name. For example, the subject common name in the certificate for youtube.com is *.google.com (this of course might change at any time). You will get more consistent results if you use the SSL Decryption policy to decrypt HTTPS traffic so that URL filtering rules work on decrypted traffic.

Note URL objects will not match HTTPS traffic if the browser resumes a TLS session because the certificate information is no longer available. So even if you carefully configure the URL object, you might get inconsistent results for HTTPS connections.

Create or Edit an FDM-Managed URL Object

URL objects are reusable components that specify a URL or IP address.

To create a URL object, follow these steps:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **URL**.

Step 3 Enter an object name and description.

Step 4 Select **Create a URL object.**

Step 5 Enter the specific URL or IP address for your object.

Step 6 Click **Add**.

Create a Firepower URL Group

A URL group can be made up of one or more URL objects representing one or more URLs or IP addresses. The Firepower Device Manager and Firepower Management Center also refer to these objects as "URL Objects."

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **URL**.

Step 3 Enter an object name and description.

Step 4 Select **Create a URL group.**

Step 5 Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding URL objects to the URL group.

Edit a Firepower URL Object or URL Group

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the details pane, click  to edit.

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Application Filter Objects

Application filter objects are used by Firepower devices. An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.

Although you can specify individual applications, application filters simplify policy creation and administration. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

You can select applications and application filters directly in a policy without using application filter objects. However, an object is convenient if you want to create several policies for the same group of applications or filters. The system includes several pre-defined application filters, which you cannot edit or delete.

Note Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

Note When an FDM-managed device is onboarded to Security Cloud Control, it converts the application filters to application filter objects without altering the rule defined in Access Rule or SSL Decryption. Because of a configuration change, the device's configuration status is changed to 'Not Synced' and requires configuration deployment from Security Cloud Control. In general, FDM does not convert the application filters to application filter objects until you manually save the filters.

Related Information:

- Create and Edit a Firepower Application Filter Object
- Deleting Objects

Create and Edit a Firepower Application Filter Object

An application filter object allows you to target hand-picked applications or a group of applications identified by the filters. This application filter objects can be used in policies.

Create a Firepower Application Filter Object

To create an application filter object, follow this procedure:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

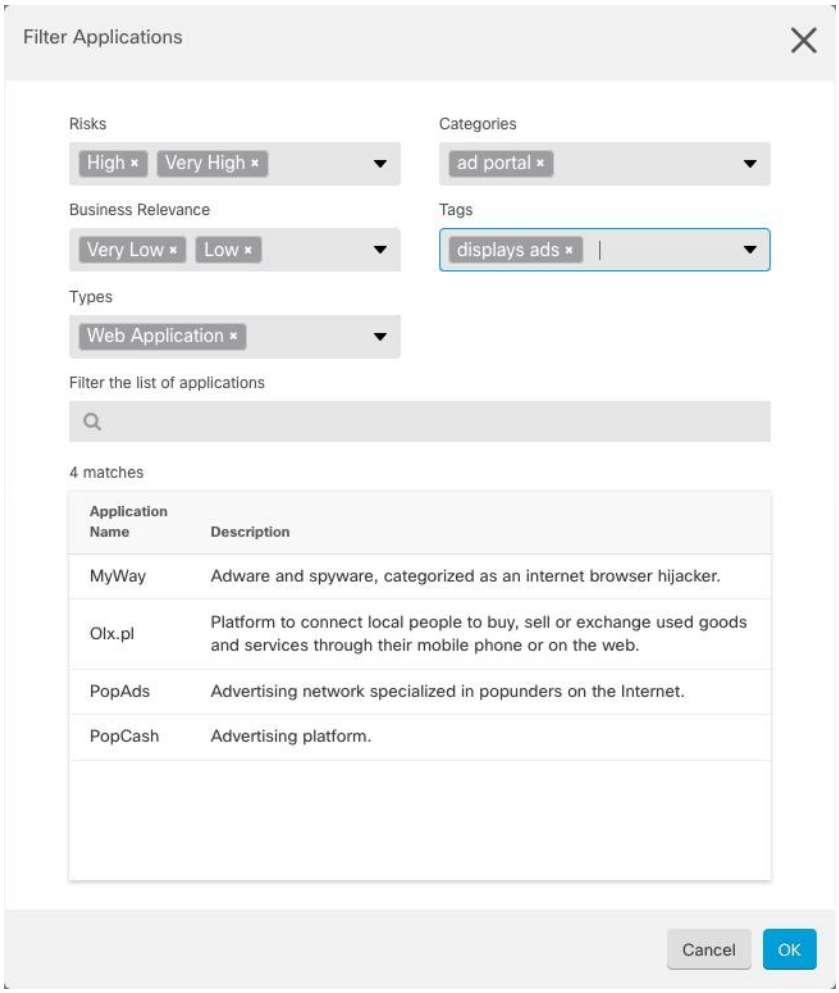
Step 2 Click **Create Object > FTD > Application Service**.

Step 3 Enter an **object name** for the object and optionally, a **description**.

Step 4 Click **Add Filter** and select the applications and filters to add to the object.

The initial list shows applications in a continually scrolling list. Click **Advanced Filter** to see the filter options and to get an easier view for selecting applications. Click **Add** when you have made your selections. You can repeat the process to add additional applications or filters.

Note Multiple selections within a single filter criteria have an OR relationship. For example, Risk is High OR Very High. The relationship between filters is AND, so Risk is High OR Very High, AND Business Relevance is Low OR Very Low. As you select filters, the list of applications in the display updates to show only those that meet the criteria. You can use these filters to help you find applications that you want to add individually, or to verify that you are selecting the desired filters to add to the rule.



Risks: The likelihood that the application is used for purposes that might be against your organization's security policy, from very low to very high.

Business Relevance: The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally, from very low to very high.

Types: The type of application.

- **Application Protocol:** Application protocols such as HTTP and SSH, which represent communications between hosts.

- **Client Protocol:** Clients such as web browsers and email clients, which represent software running on the host.
- **Web Application:** Web applications such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic.

Categories: A general classification for the application that describes its most essential function.

Tags: Additional information about the application, similar to category.

For encrypted traffic, the system can identify and filter traffic using only the applications tagged SSL Protocol. Applications without this tag can only be detected in unencrypted or decrypted traffic. Also, the system assigns the decrypted traffic tag to applications that the system can detect in decrypted traffic only, not encrypted or unencrypted.

Applications List (bottom of the display): This list updates as you select filters from the options above the list, so you can see the applications that currently match the filter. Use this list to verify that your filter is targeting the desired applications when you intend to add filter criteria to the rule. To add a specific application or applications to your object, select them from the filtered list. Once you select the applications, the filter will no longer apply. If you want the filter itself to be the object, do not select an application from the list. Then the object will represent ever application identified by the filter.

Step 5 Click **OK** to save your changes.

Edit a Firepower Application Filter Object

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon in the Actions pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 6 Click **Save**.

Step 7 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Related Information:

- Objects
- Object Filters
- Deleting Objects

Geolocation Objects

A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses. For example,

using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

You can typically select geographical locations directly in a policy without using geolocation objects. However, an object is convenient if you want to create several policies for the same group of countries and continents.

Update Geolocation Database

To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB). At this time, this is not a task that you can perform using Security Cloud Control. See the following sections of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running to learn more about the GeoDB and how to update it.

- Updating System Databases and Feeds
- Updating System Databases

Create and Edit a Firepower Geolocation Filter Object

You can create a geolocation object by itself on the object page or when creating a security policy. This procedure creates a geolocation object from the object page.

To create a geolocation object, follow these steps:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **Geolocation**.

Step 3 Enter an **object name** for the object and optionally, a **description**.

Step 4 In the filter bar, start typing the name of a country or a region and you are presented with a list of possible matches.

Step 5 Check the country, countries, or regions that you want to add to the object.

Step 6 Click **Add**.

Edit a Geolocation Object

Procedure

Step 1 In the left pane, choose **Objects > FDM Objects**.

Step 2 Use the filter panes and search field to locate your object.

Step 3 In the **Actions** pane, click **Edit**.

Step 4 You can change the name of the object and add or remove countries and regions to your object.

Step 5 Click **Save**.

Step 6 You will be notified if any devices are impacted. Click **Confirm**.

Step 7 If a device or policy was impacted, open the **Inventory** page and **Preview and Deploy** the changes to the device.

DNS Group Objects

Domain Name System (DNS) groups define a list of DNS servers and some associated attributes. DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.

FDM-managed devices must have a DNS server configured prior to creating a new DNS Group Object. You can either add a DNS Server to theConfigure DNS Server in Security Cloud Control or create a DNS server in firewall device manager and then sync the FDM-managed configuration to Security Cloud Control. To create or modify the DNS server settings in firewall device manager, see **Configuring DNS for Data and Management Interfaces** in the Cisco Firepower Device Manager Configuration Guide, Version 6.4. or later.

Create a DNS Group Object

Use the following procedure to create a new DNS group object in Security Cloud Control:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **DNS Group**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Enter the IP address of a **DNS server**. You can add up to six DNS servers; click the **Add DNS Server**. If you want to remove a server address, click the delete icon.

Note The list is in priority order: the first server in the list is always used, and subsequent servers are used only if a response is not received from the servers above it. Although you can add up to six servers, only the first 3 servers listed will be used for the management interface.

Step 7 Enter the **Domain Search Name**. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

Step 8 Enter the amount of **Retries**. The number of times, from 0 to 10, to retry the list of DNS servers when the system does not receive a response. The default is 2. This setting applies to DNS groups used on the data interfaces only.

Step 9 Enter the **Timeout** value. The number of seconds, from 1 to 30, to wait before trying the next DNS server. The default is 2 seconds. Each time the system retries the list of servers, this timeout doubles. This setting applies to DNS groups used on the data interfaces only.

Step 10 Click **Add**.

Edit a DNS Group Object

You can edit a DNS group object that was created in Security Cloud Control or in firewall device manager. Use the following procedure to edit an existing DNS group object:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the **DNS Group Object** you want to edit by using object filters and search field.

Step 3 Select the object and click the edit icon in the **Actions** pane.

Step 4 Edit any of the following entries:

- Object Name.
- Description.
- DNS Server. You can edit, add, or remove DNS servers from this list.
- Domain Search Name.
- Retries.
- Timeout.

Step 5 Click **Save**.

Step 6 Preview and Deploy Configuration Changes for All Devices.

Delete a DNS Group Object

Use the following procedure to delete a DNS Group Object from Security Cloud Control:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the **DNS Group Object** you want to edit by using object filters and search field.

Step 3 Select the object and click the **Remove** icon.

Step 4 Confirm you want to delete the DNS group object and click **Ok**.

Step 5 Preview and Deploy Configuration Changes for All Devices.

Add a DNS Group Object as an FDM-Managed DNS Server

You can add a DNS group object as the preferred DNS Group for either the **Data Interface** or the **Management Interface**. See FDM-Managed Device Settings for more information.

Certificate Objects

Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

See the **About Certificates** and **Configuring Certificates** following sections of the Resuable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

About Certificates

Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

You can create the following types of certificate:

- **Internal certificates**—Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

  The system comes with the following pre-defined internal certificates, which you can use as is or replace: **DefaultInternalCertificate** and **DefaultWebServerCertificate**

- **Internal Certificate Authority (CA)** certificates—Internal CA certificates are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

  The system comes with the following pre-defined internal CA certificate, which you can use as is or replace: **NGFW-Default-InternalCA**

- **Trusted Certificate Authority (CA)** certificates—A trusted CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

  Certificate Authorities (CAs) are trusted authorities that "sign" certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization. CAs are responsible for managing certificate requests and issuing digital certificates.

  The system includes many trusted CA certificates from third party Certificate Authorities. These are used by SSL decryption policies for Decrypt Re-Sign actions.

For more information, see the **Certificate Types Used by Feature** section of the Reusable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Certificate Types Used by Feature

You need to create the right type of certificate for each feature. The following features require certificates.

Identity Policies (Captive Portal)—Internal Certificate

(Optional.) Captive portal is used in identity policies. Users must accept this certificate when authenticating to the device for purposes of identifying themselves and receiving the IP address associated with their usernames. If you do not supply a certificate, the device uses an automatically generated certificate.

SSL Decryption Policy—Internal, Internal CA, and Trusted CA Certificates.

(Required.) The SSL decryption policy uses certificates for the following purposes:

- Internal certificates are used for known key decryption rules.
- Internal CA certificates are used for decrypt re-sign rules when creating the session between the client and FDM-managed device.
- Trusted CA certificates
  - They are used indirectly for decrypt re-sign rules when creating the session between the FDM-managed device and server. Unlike the other certificates, you do not directly configure these certificates in the SSL decryption policy; they simply need to be uploaded to the system. The system includes a large number of trusted CA certificates, so you might not need to upload any additional certificates.
  - When creating an Active Directory Realm object and configuring the directory server to use encryption.

Configuring Certificates

Certificates used in identity policies or SSL decryption policies must be an X509 certificate in PEM or DER format. You can use OpenSSL to generate certificates if needed, obtain them from a trusted Certificate Authority, or create self-signed certificates.

Use these procedures to configure certificate objects:

- Uploading Internal and Internal CA Certificates
- Uploading Trusted CA Certificates
- Generating Self-Signed Internal and Internal CA Certificates
- To view or edit a certificate, click either the edit icon or the view icon for the certificate.
- To delete an unreferenced certificate, click the trash can icon (delete icon) for the certificate. See Deleting Objects.

Uploading Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

For information on the features that use these certificates, see Certificate Types Used by Feature.

Procedure

This procedure creates an internal or internal CA certificate by uploading a certificate file or pasting existing certificate text into a text box. If you want to generate a self signed certificate, see Generating Self-Signed Internal and Internal CA Certificates.

To create an internal or internal CA certificate object, or when adding a new certificate object to a policy, follow this procedure:

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:
  a. In the left pane, click **Objects > FDM Objects**.
  b. Click the plus button and select **FTD** > **Certificate**
- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **Internal Certificate** or **Internal CA.**

Step 4 In step 2, select **Upload** to upload the certificate file.

Step 5 In step 3, in the **Server Certificate** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard. If you paste the certificate into the text box, the certificate must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

Step 6 In step 3, in the **Certificate Key** area, paste the key contents into the Certificate Key text box or upload the key file as explained in the wizard. If you paste the key into the text box, the key must include the BEGIN PRIVATE KEY or BEGIN RSA PRIVATE KEY and END PRIVATE KEY or END PRIVATE KEY lines.

Note The key cannot be encrypted.

Step 7 Click **Add**.

Uploading Trusted CA Certificates

A trusted Certificate Authority (CA) certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

For information on the features that use these certificates, see Certificate Types Used by Feature.

Obtain a trusted CA certificate from an external certificate authority, or create one using your own internal CA, for example, with OpenSSL tools. Then, use the following procedure to upload the certificate.

Procedure

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:
  a. In the left pane, click **Objects > FDM Objects**.
  b. Click the plus button and select **FTD** > **Certificate**.
- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **External CA Certificate** and click **Continue**. The wizard advances to step 3.

Step 4 In step 3, in the **Certificate Contents** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard.

The certificate must follow these guidelines:

- The name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.
- The certificate must be an X509 certificate in PEM or DER format.
- The certificate you paste must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

Step 5 Click **Add**.

Generating Self-Signed Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

You can also create these certificates using OpenSSL, or obtain them from a trusted CA, and upload them. For more information, see Uploading Internal and Internal CA Certificates.

For information on the features that use these certificates, see Certificate Types Used by Feature.

Note New self-signed certificates are generated with a 5-year validity term. Be sure to replace certificates before they expire.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Procedure

This procedure generates a self-signed certificate by entering the appropriate certificate field values in a wizard. If you want to create an internal or internal CA certificate by uploading a certificate file, see Uploading Internal and Internal CA Certificates.

To generate a self-signed certificate, follow this procedure:

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:
  a. In the left pane, click **Objects > FDM Objects**.
  b. Click the plus button and select **FTD** > **Certificate**.
- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **Internal Certificate** or **Internal CA.**

Step 4 In step 2, select **Self-Signed** to create the self-signed certificate in this step.

Step 5 Configure at least one of the following for the certificate subject and issuer information.

- Country (C)— Select the country code from the drop-down list.
- State or Province (ST)— The state or province to include in the certificate.
- Locality or City (L)— The locality to include in the certificate, such as the name of the city.
- Organization (O)— The organization or company name to include in the certificate.
- Organizational Unit (Department) (OU)— The name of the organization unit (for example, a department name) to include in the certificate.
- Common Name (CN)— The X.500 common name to include in the certificate. This could be the name of the device, web site, or another text string. This element is usually required for successful connections. For example, you must include a CN in the internal certificate used for remote access VPN.

Step 6 Click **Add**.

About IPsec Proposals

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.
- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

The following topics explain how to configure IPsec proposals for each IKE version:

Managing an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Security Cloud Control supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

Related Topics

Create an IKEv1 IPsec Proposal Object, on page 441

Create or Edit an IKEv1 IPsec Proposal Object

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button and select **FTD** > **IKEv1 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Select the Mode in which the IKEv1 IPsec Proposal object operates.

- **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that

both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Step 5 Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 422.

Step 6 Select the **ESP Hash** or integrity algorithm to use for authentication. For an explanation of the options, see Deciding Which Hash Algorithms to Use, on page 423.

Step 7 Click **Add**.

Managing an IKEv2 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

Related Topics

Create or Edit an IKEv2 IPsec Proposal Object, on page 442

Create or Edit an IKEv2 IPsec Proposal Object

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv2 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Configure the IKE2 IPsec proposal objects:

- **Encryption**—The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 422.

- **Integrity Hash**—The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use, on page 423.

Step 5 Click **Add**.

About Global IKE Policies

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

The following procedure explains how to configure the global policy through the Objects page. You can also enable, disable, and create policies when editing a VPN connection by clicking Edit for the IKE Policy settings.

The following topics explain how to configure IKE policies for each version:

- Managing IKEv1 Policies
- Managing IKEv2 Policies

Managing IKEv1 Policies

About IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv1 Policy, on page 437

Create or Edit an IKEv1 Policy

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv1 Policy** to create a new IKEv1 policy.
- In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv1 properties.

- **Priority**—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **Encryption**—The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group**—The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Lifetime**—The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).
- **Authentication**—The method of authentication to use between the two peers. For more information, see Deciding Which Authentication Method to Use, on page 424.
  - **Preshared Key**—Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate**—Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer.

The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.

- **Hash**—The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 422.

Step 5 Click **Add**.

Managing IKEv2 Policies

About IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv2 Policy, on page 439

Create or Edit an IKEv2 Policy

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv2 Policy** to create a new IKEv2 policy.
- In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv2 properties.

- **Priority**—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.

- **State**—Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption**—The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 422.
- **Diffie-Hellman Group**—The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use, on page 424.
- **Integrity Hash**—The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 422.
- **Pseudo-Random Function (PRF) Hash**—The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 422.
- **Lifetime**—The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

Step 5 Click **Add**.

RA VPN Objects

Security Zone Object

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only.

The Firepower system creates the following zones during initial configuration and they are displayed in Security Cloud Control's object page. You can edit zones to add or remove interfaces, or you can delete the zones if you no longer use them.

- **inside_zone**-Includes the inside interface. This zone is intended to represent internal networks.
- **outside_zone**-Includes the outside interface. This zone is intended to represent networks external to your control, such as the internet.

Typically, you would group interfaces by the role they play in your network. For example, you would place the interface that connects to the internet in the **outside_zone** security zone, and all of the interfaces for your internal networks in the **inside_zone** security zone. Then, you could apply access control rules to traffic coming from the outside zone and going to the inside zone.

Before creating zones, consider the access rules and other policies you want to apply to your networks. For example, you do not need to put all internal interfaces into the same zone. If you have 4 internal networks, and you want to treat one differently than the other three, you can create two zones rather than one. If you have an interface that should allow outside access to a public web server, you might want to use a separate zone for the interface.

Related Information:

- Create or Edit a Firepower Security Zone Object
- Assign a Firepower Interface to a Security Zone
- Deleting Objects

Create or Edit a Firepower Security Zone Object

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only. For more information see,Security Zone Object.

A security zone object is not associated with a device unless it is used in a rule for that device.

Create a Security Zone Object

To create a security zone object, follow these instructions:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button  and select **FTD** > **Security Zone** to create the object.

Step 3 Give the object a name and, optionally, a description.

Step 4 Select the interfaces to put in the security zone.

Step 5 Click **Add.**

Edit a Security Zone Object

After onboarding an FDM-managed device, you will find there are already at least two security zones, one is the inside_zone and the other is the outside_zone. These zones can be edited or deleted. To edit any security zone object, follow these instructions:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Find the object you want to edit:

- If you know the name of the object, you can search for it in the Objects page:
  - Filter the list by security zone.
  - Enter the name of the object in the search field.
  - Select the object.
- If you know the object is associated with a device, you can search for it starting on the **Inventory** page.
  - In the navigation pane, click **Inventory**.
  - Click the **Devices** tab.
  - Click the apporpriate tab.
  - Use the device Filters and Page Level Search bar to locate your device.
  - Select the device.
  - In the Management pane at the right, click  **Objects.**
  - Use the object filter and search bar to locate the object you are looking for.

Note If the security zone object you created is not associated with a rule in a policy for your device, it is considered "unassociated" and you will not see it among the search results for a device.

Step 3 Select the object.

Step 4 Click the **Edit** icon in the Actions pane at the right.

Step 5 After editing any of the attributes of the object. Click **Save**.

Step 6 After clicking Save you receive a message explaining how these changes will affect other devices. Click **Confirm** to save the changes or **Cancel**.

Service Objects

Firepower Service Objects

FTD service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the IP protocol suite.

FTD service groups are collections of service objects. A service group may contain objects for one or more protocols. You can use the objects and groups in security policies for purposes of defining network traffic matching criteria, for example, to use access rules to allow traffic to specific TCP ports. The system includes

several pre-defined objects for common services. You can use these objects in your policies; however, you cannot edit or delete system-defined objects.

Firepower Device Manager and Firepower Management Center refer to service objects as port objects and service groups and port groups.

See Create and Edit Firepower Service Objects for more information.

Protocol Objects

Protocol objects are a type of service object that contain less-commonly used or legacy protocols. Protocol objects are identified by a name and protocol number. Security Cloud Control recognizes these objects in ASA and Firepower (FDM-managed device) configurations and gives them their own filter of "Protocols" so you can find them easily.

See Create and Edit Firepower Service Objects for more information.

ICMP Objects

An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. Security Cloud Control recognizes these objects in ASA and Firepower configurations when those devices are onboarded and Security Cloud Control gives them their own filter of "ICMP" so you can find the objects easily.

Using Security Cloud Control, you can rename or remove ICMP objects from an ASA configuration. You can use Security Cloud Control to create, update, and delete ICMP and ICMPv6 objects in a Firepower configuration.

Note For the ICMPv6 protocol, AWS does not support choosing specific arguments. Only rules that allow all ICMPv6 messages are supported.

See Create and Edit Firepower Service Objects for more information.

Related Information:

- Deleting Objects, on page 116

Create and Edit Firepower Service Objects

To create a firepower service object, follow these steps:

firewall device manager (FDM-managed) service objects are reusable components that specify a TCP/IP protocol and a port. The firewall device manager, On-Premises Firewall Management Center and Cloud-delivered Firewall Management Center refer to these objects as "Port Objects."

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click the blue button  on the right to create an object, and select **FTD > Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service object.**

Step 5 Click the **Service Type** button and select the protocol for which you want to create an object.

Step 6 Configure the protocol as follows:

- **TCP**, **UDP**
  - Select **eq** and then enter either a port number or a protocol name. For example, you could enter 80 as a port number or HTTP as the protocol name.
  - You can also select **range** and then enter a range of port numbers, for example, **1 65535** (to cover all ports).
- **ICMP**, **IPv6-ICMP**-Select the ICMP **Type.** Select **Any** for the type to apply to all ICMP messages. For information on the types and codes, see the following pages:
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other**-Select the desired protocol.

Step 7 Click **Add**.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Create a Firepower Service Group

A service group can be made up of one or more service objects representing one or more protocols. The service objects need to be created before they can be added to the group. The Firepower Device Manager and Firepower Management Center refer to these objects as "Port Objects."

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click the blue button  on the right to create an object, and select **FTD > Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service group.**

Step 5 Add an object to the group by clicking **Add Object.**

- Click **Create** to create a new object as you did above in Create and Edit Firepower Service Objects above.
- Click **Choose** to add an existing service object to the group. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding service objects to the service group.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Edit a Firepower Service Object or Service Group

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the Actions pane, click **Edit** .

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Security Group Tag Group

Security Group Tags

About Security Group Tags

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria. Thus, you can block or allow access based on security group membership rather than IP addresses.

In ISE, you can create a SGT and assign host or network IP addresses to each tag. If you assign an SGT to a user's account, the SGT is assigned to the user's traffic. After you configure FDM-managed device to connect to an ISE server and create the SGT, you can create SGT groups in Security Cloud Control and build access control rules around them. Note that you must configure ISE's SGT Exchange Protocol (SXP) mapping before you can associate an SGT to an FDM-managed device. See **Security Group Tag Exchange Protocol** in the Cisco Identity Services Engine Administrator Guide of the version you are currently running for more information.

When an FDM-managed device evaluates SGT as a traffic matching criteria for an access control rule, it uses the following priority:

1. The source SGT defined in the packet, if any. No destination matching is done using this technique. For the SGT to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
2. The SGT assigned to the user session, as downloaded from the ISE session directory. You need to enable the option to listen to session directory information for this kind of SGT matching, but this option is on by default when you first create the ISE identity source. The SGT can be matched to source or destination. Although not required, you would also normally set up a passive authentication identity rule, using the ISE identity source along with an AD realm, to collect user identity information.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is within the range for an SGT, then the traffic matches the access control rule that uses the SGT. The SGT can be matched to source or destination.

Note You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on a relevant collections of tags if that is appropriate.

Version Support

Security Cloud Control currently supports SGT and SGT groups on FDM-managed devices running Version 6.5 and later. an FDM-managed device allows you to configure and connect to an ISE server in Version 6.5 and later but not does not support SGT configuration in the UI until Version 6.7.

From the FDM-managed UI, this means that an FDM-managed device running Version 6.5 or later can download SXP mappings of SGTs but cannot be manually added to objects or access control rules. To make changes to the SGTs for devices running Version 6.5 or Version 6.6, you must use the ISE UI. If the device running Version 6.5 is onboarded to Security Cloud Control, however, you can see the current SGTs associated with the device and create SGT groups.

SGT in Security Cloud Control

Security Group Tags

SGTs are read-only in Security Cloud Control. You cannot create or edit an SGT in Security Cloud Control. To create an SGT, see the Cisco Identity Services Engine Administrator Guide of the version your are currently running.

SGT Groups

Note An FDM-managed device refers to groups of SGTs as SGT dynamic objects. In Security Cloud Control, these lists of tags are currently called SGT groups. You can create an SGT group in Security Cloud Control without referring to the FDM-managed device or ISE UI.

Use SGT groups to identify source or destination addresses based on an SGT assigned by ISE. You can then use the objects in access control rules for purposes of defining traffic matching criteria. You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information.

Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

In order to create an SGT group in Security Cloud Control, you must have at least one SGT already configured and SGT mappings from an ISE server configured for the FDM-managed console of the device you want to use. Note that if more than one FDM-managed device is associated with the same ISE server, an SGT or SGT group can be applied to more than one device. If a device is not associated with an ISE server, you cannot include SGT objects in your access control rule, or apply an SGT group to that device configuration.

SGT Groups in Rules

SGT groups can be added to access control rules; they appear as source or destination network objects. For more information about how networks work in rules, see Source and Destination Criteria in an FDM-Managed Access Control Rule.

You can create an SGT group from the Objects page. See Create an SGT Group, on page 154 for more information.

Create an SGT Group

To create an SGT group that can be used for an access control rule, use the following procedure:

Before you begin

You must have the following configurations or environments configured prior to creating a security group tag (SGT) group:

- FDM-managed device must be running at least Version 6.5.
- You must configure the ISE identity source to subscribe to SXP mappings and enable deploy changes. To manage SXP mappings, see **Configure Security Groups and SXP Publishing in ISE** of the Firepower Device Manager Configuration Guide for the version you're using, Version 6.7 and later.
- All SGTs must be created in ISE. To create an SGT, see the Cisco Identity Services Engine Configuration Guide of the version your are currently running.

Procedure

Step 1 On the left pane, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD > Network**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Click **SGT** and use the drop-down menu to check all the applicable SGTs you want included in the group. You can sort the list by SGT name.

Step 7 Click **Save**.

Note You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Edit an SGT Group

To edit an SGT group, use the following procedure:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the SGT group you want to edit by using object filters and search field.

Step 3 Select the SGT group and click the edit icon in the **Actions** pane.

Step 4 Modify the SGT group. Edit the name, description, or the SGTs associated with the group.

Step 5 Click **Save**.

Note You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Add an SGT Group to an Access Control Rule

To add an SGT group to an access control rule, use the following procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to add the SGT group to.

Step 4 In the**Management** pane, select **Policy**.

Step 5 Click the blue plus button for either the **Source** or **Destination** objects and select **SGT Groups**.

Step 6 Locate the SGT group(s) you want to edit by using object filters and search field.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices.

Note If you need to create an additional SGT group, click **Create New Object**. Fill in the required information mentioned in Create an SGT Group and **Add** the SGT group to the rule.

Syslog Server Objects

FDM-managed devices have a limited capacity to store events. To maximize storage for events, you can configure an external server. A system log (syslog) server object identifies a server that can receive connection-oriented or diagnostic syslog messages. If you have a syslog server set up for log collection and analysis, you can use the Security Cloud Control to create objects to define them and use the objects in the related policies.

Create and Edit Syslog Server Objects

To create a new syslog server object, follow these steps:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click the **Create Object** button  .

Step 3 Select **Syslog Server** under FDM-managed device object types

Step 4 Configure the syslog server object properties:

- **IP Address**—Enter the IP address of the syslog server.
- **Protocol Type**—Select the protocol that your syslog server uses to receive messages. If you select TCP, the system can recognize when the syslog server is not available, and stops sending events until the server is available again.
- **Port Number**—Enter a valid port number to use for syslog. If your syslog server uses default ports, enter 514 as the default UDP port or 1470 as the default TCP port. If the server does not use default ports, enter the correct port number. The port must be in the range 1025 to 65535.
- **Select an interface**—Select which interface should be used for sending diagnostic syslog messages. Connection and intrusion events always use the management interface. Your interface selection determines the IP address associated with syslog messages. Note that you can only select **one** of the options listed below. You cannot select both. Select one of the following options:
  - **Data Interface**—Use the data interface you select for diagnostic syslog messages. Select an interface from the generated list. If the server is accessible through a bridge group member interface, select the bridge group interface (BVI). If it is accessible through the Diagnostic interface (the physical management interface), we recommend that you select Management Interface instead of this option. You cannot select a passive interface. For connection and intrusion syslog messages, the source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.
  - **Management Interface**—Use the virtual management interface for all types of syslog messages. The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

Step 5 Click **Add**.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit Syslog Server Objects

To edit an existing syslog server object, follow these steps:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the desired syslog server object and select it. You can **filter** the object list by the syslog server object type.

Step 3 In the Actions pane, click **Edit**.

Step 4 Make the desired edits and click **Save**.

Step 5 Confirm the changes you made.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Deleting Objects

Create a Syslog Server Object for Secure Logging Analytics (SaaS)

Create a syslog server object with the IP address, TCP port, or UDP port of the Secure Event Connector (SEC) you want to send events to. You would create one syslog object for every SEC that you have onboarded to your tenant but you would only send events from one rule to one syslog object representing one SEC.

Prerequisite

This task is part of a larger workflow. See Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices, on page 614 before you begin.

Procedure

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Click the **Create Object** button .

Step 3 Select **Syslog Server** under FDM-managed device object types.

Step 4 Configure the syslog server object properties. To find these properties of the SEC, from the navigation pane on the left, choose **Tools & Services** > **Secure Connectors**. Then select the Secure Event Connector you want to configure the syslog object for and look in the Details pane on the right.

- **IP Address**—Enter the IP address of the SEC.
- **Protocol Type**—Select TCP or UDP.
- **Port Number**—Enter port 10125 if you selected TCP or 10025 if you selected UDP.
- **Select an interface**—Select the interface configured to reach the SEC.

Note FDM-managed device supports one syslog object per IP address so you will have to choose between using TCP and UDP.

Step 5 Click **Add**.

What to do next

Continue with Step 3 of Existing Security Cloud Control Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud.

Manage Security Policies in Security Cloud Control

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use Security Cloud Control to configure security policies on many different types of devices.

- FDM Policy Configuration, on page 328
- Network Address Translation, on page 407

FDM Policy Configuration

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. Use Security Cloud Control to manage all the components of FDM-managed device's security policies.

FDM-Managed Access Control Policy

You can use Security Cloud Control to manage the access control policy of an FDM-managed device. The access control policy controls access to network resources by evaluating network traffic against access control rules. The FDM-managed device compares the criteria of the access control rules, in the order they appear in the access control policy, to the network traffic. When all the traffic conditions in an access control rule are

- **Trust**—Allow traffic without further inspection of any kind.
- **Allow**—Allow the traffic subject to the intrusion and other inspection settings in the policy.
- **Block**—Drop the traffic unconditionally. The traffic is not inspected.

If none of the rules in the access control policy match the network traffic, the FDM-managed device takes the default action listed below the access control rules.

Read an FDM-Managed Access Control Policy

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

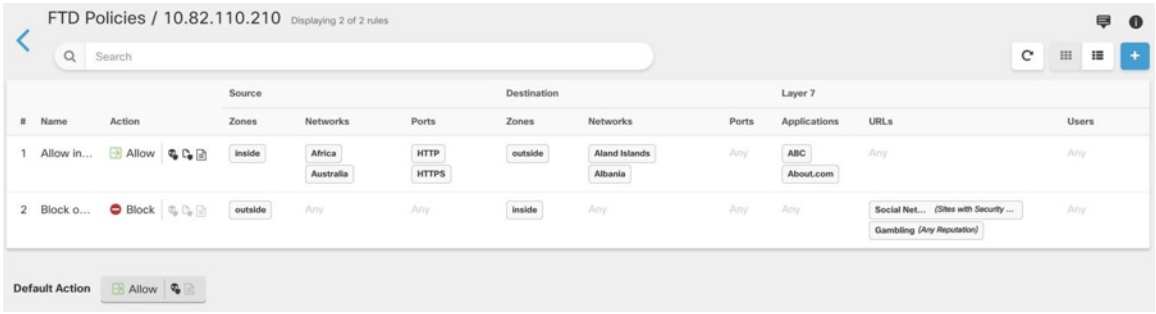
Step 3 Click the **FTD** tab and select the device whose policy it is you want to read.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 To ensure that you see the whole policy, click **Show All** in the Filter panel.

Step 6 Toggle the rule column display to view the rules with more or fewer column. If you are used to viewing access control rules in an FDM-managed device, toggle the rule column display to show more columns.

Here is an example of how to read a rule in a policy. All traffic is evaluated against rule 1 first for a match. If the traffic matches rule 1, the action for that rule is applied to the traffic. Traffic that originates from the inside zone, AND originates from Africa OR Australia, AND originates from HTTP or HTTPS ports, AND arrives at the outside zone, AND arrives at the Aland Islands OR Albania, AND arrives at any port, AND arrives at ABC OR About.com is allowed to flow from the source to the destination. We can also see that an intrusion policy and a file policy are applied to the rule and that events from the rule are being logged.



Related Information:

- Configure the FDM Access Control Policy

Configure the FDM Access Control Policy

FDM-managed devices have a single policy. A section of that policy has access control rules. For ease of discussion, we refer to the section of the policy that has access control rules as the *access control policy*. After onboarding the FDM-managed device, you add rules to, or edit rules in, the access control policy.

If you are onboarding a new FDM-managed device, it may be that there are no rules in the policy that was imported. In that case, when you open the FDM Policy page, you will see the message, "No results found." If you see that message, you can start adding rules to the FDM-Managed Device Policy and then deploy them to the device from Security Cloud Control.

Tips Before you Begin

When adding conditions to access control rules, consider the following tips:

- You can create custom objects for some of the conditions at the time you add them to the rule. Look in the dialog boxes for a link to create custom objects.
- You can configure multiple conditions per rule. Traffic must match all the conditions in the rule for the rule to apply to traffic. For example, you can use a single rule to perform URL filtering for specific hosts or networks.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches any of a condition's criteria satisfies the condition. For example, you can use a single rule to apply application control for up to 50 applications or application filters. Thus, there is an OR relationship among the items in a single condition, but an AND relationship between condition types (for example, between source/destination and application).
- Some features require that you have enabled the appropriate Firepower licenses.
- Some editing tasks may not require you to enter the edit mode. From the policy page, you can modify a condition in the rule by clicking the + button within that condition column and select the desired object or element in the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

Create or Edit an FDM-Managed Access Control Policy

Use this procedure to edit an FDM-managed access control policy using Cisco Security Cloud Control:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and whose access control whose policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Do any of the following:

- To create a new rule, click the blue plus button  .
- To edit an existing rule, select the rule and click the edit icon in the **Actions** pane. (Simple edits may also be performed inline without entering edit mode.)
- To delete a rule you no longer need, select the rule and click the remove icon in the Actions pane.
- To move a rule within the policy, select the rule in the access control table and click the up or down arrow at the end of the rule row to move the rule.

When editing or adding a rule, continue with the remaining steps in this procedure.

Step 6 In the **Order** field, select the position for the rule within the policy. Network traffic is evaluated against the list of rules in numerical order, 1 to "last."

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 7 Enter the rule name. You can use alphanumeric characters, spaces, and these special characters: + . _ -

Step 8 Select the action to apply if the network traffic is matched by the rule:

- **Trust**—Allow traffic without further inspection of any kind.
- **Allow**—Allow the traffic subject to the intrusion and other inspection settings in the policy.
- **Block**—Drop the traffic unconditionally. The traffic is not inspected.

Step 9 Define the traffic matching criteria by using any combination of attributes in the following tabs:

- **Source**—Click the **Source** tab and add or remove security zones (interfaces), networks (which include networks, continents, and custom geolocations), or ports from which the network traffic originated. The default value is "Any."
- **Destination**—Click the **Destination** tab and add or remove the security zones (interfaces), networks (which include networks, continents and custom geolocations), or ports on which the traffic arrives. The default value is "Any." See Source and Destination Criteria in an FDM-Managed Access Control Rule.
- **Applications**—Click the **Application** tab and add or remove a web application, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application. See Application Criteria in an FDM-Managed Access Control Rule
- **URLs**—Click the **URL** tab and add or remove a URL or URL category of a web request. The default is any URL. See URL Conditions in an FDM-Managed Access Control Rule to learn how to fine-tune this condition using URL categories and reputation filters.
- **Users**—Active Directory realm objects, special identities (failed authentication, guest, no authentication required, unknown), and user groups added to the rule from firewall device manager are visible in the rule row but it is not yet editable in Security Cloud Control.

  Caution Individual user-objects are not yet visible in an access control policy rule in Security Cloud Control. Log in to an FDM-managed device to see how an individual user-object may affect an access control policy rule.

Step 10 (Optional, for rules with the Allow action) Click the **Intrusion Policy** tab to assign an intrusion inspection policy to inspect traffic for intrusions and exploits. See Intrusion Policy Settings in an FDM-Managed Access Control Rule.

a. **To log Intrusion events** generated by intrusion policy rules, see " FDM-Managed Device Settings" for the device.

Step 11 (Optional, for rules with the Allow action) Click the **File Policy** tab to assign a file policy that inspects traffic for files that contain malware and for files that should be blocked. See File Policy Settings in an FDM-Managed Access Control Rule.

a. **To log file events** enerated by file policy rules, see "FDM-Managed Device Settings" for the device.

Step 12 (Optional) Click the logging tab to enable logging and collect **connection events** reported by the access control rule.

See Logging Settings in an FDM-Managed Access Control Rule for more information on logging settings.

If you subscribe to Cisco Security Analytics and Logging, you can configure connection events in Security Cloud Control and send them to the Secure Event Connector (SEC) by Create a Syslog Server Object for Secure Logging Analytics (SaaS). See Secure Logging Analytics for FDM-Managed Devices for more information about this feature. You would create one syslog object for every SEC that you have onboarded to your tenant, but you would only send events generated by one rule, to one syslog object, representing one SEC.

Step 13 Click **Save**. You are now done configuring a specific rule in the security policy.

Step 14 You can now configure the **Default Action** for the security policy as a whole. The Default Action defines what happens if network traffic does not match any of the rules in the access control policy, intrusion policy, or file/malware policy.

Step 15 Click the Default Action for the policy.

Step 16 Configure an intrusion policy as you did in step 9, above.

Step 17 Configure logging connection events generated by the Default Action.

If you subscribe to Cisco Security Analytics and Logging, you can send events generated by the default action to a Secure Event Connector (SEC) by Create a Syslog Server Object for Secure Logging Analytics (SaaS). See Secure Logging Analytics for FDM-Managed Devices for more information about this feature. You would create one syslog object for every SEC that you have onboarded to your tenant, but you would only send events generated by rule to one syslog object, representing one SEC.

Step 18 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 19 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configuring Access Policy Settings

You can configure settings that apply to the access policy, rather than to specific rules within the policy.

Procedure

These settings apply to the access policy as a whole, rather than to specific rules within the policy.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and whose access control whose policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Click the **Settings** icon and configure these settings:

- **TLS Server Identity Discovery** - TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate.

We recommend that you enable this option to ensure encrypted connections are matched to the right access control rule. The setting decrypts the certificate only; the connection remains encrypted. Enabling this option is sufficient to decrypt TLS 1.3 certificates; you do not need to create a corresponding SSL decryption rule. Available for FDM-managed devices running software version 6.7 or later.

- **Reputation Enforcement on DNS Traffic** - Enable this option to apply your URL filtering category and reputation rules to DNS lookup requests. If the fully-qualified domain name (FQDN) in the lookup request has a category and reputation that you are blocking, the system blocks the DNS reply. Because the user does not receive a DNS resolution, the user cannot complete the connection. Use this option to apply URL category and reputation filtering to non-web traffic. For more information, see DNS Request Filtering. Available for FDM-managed devices running software version 7.0 and later.

Step 6 Click **Save**.

About TLS Server Identity Discovery

Typically, the TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable early application detection and URL categorization to ensure encrypted connections are matched to the right access control rule. This setting decrypts the certificate only; the connection remains encrypted.

Note This feature is currently available for FDM-managed devices running on software version 6.7 or later.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and whose access control whose policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Click the settings button.

Step 6 Click the slider next to **TLS Server Identity Discovery** to enable early application detection and URL categorization for encrypted connections.

Step 7 Click **Save**.

Copy FDM-Managed Access Control Rules

Use this procedure to copy access control rules by copying it from their current position and pasting them to a new position in the same policy or by pasting them to the policy of a different FDM-managed device. You can paste the rule before or after other rules in the policy, so the rule evaluates that network traffic in its proper order within the policy.

Copy Rules within the Device

To copy rules within an FDM-managed device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device you whose policy it is you want to edit.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to copy and click **Copy** in the **Actions** pane on the right.

Step 6 In the policy where you want to paste the rule(s), select the rule that your copied rule(s) should precede or follow and, in the **Actions** pane, click one fo the following options:

- **Paste Before**automatically pastes one or more copied rules above the selected rule, so the copied rule is ordered above it.
- **Paste After**automatically pastes one or more copied rules below the selected rule, so the copied rule is ordered below it.

The paste operation can be performed multiple times at any required position.

Note When pasting rules within an FDM-managed device, if a rule with the same name exists, '- Copy' is appended to the original name. If the renamed name also exists, '- Copy n' is appended to the original name. For example, 'rule name - Copy 2'.

Step 7 Review your changes and Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device now or wait and deploy multiple changes at once.

Copy Rules from One FDM-Managed Device Policy to Another FDM-Managed Device Policy

When copying rules from one FDM-managed device policy to another FDM-managed device policy, objects associated with those rules are copied to the new FDM-managed device as well.

Security Cloud Control validates some conditions when pasting the rules. For more information, see Behavior of Objects when Pasting Rules to Another Device.

Important **Important**: Security Cloud Control allows you to copy rules from one FDM-managed device to another FDM-managed device only if the same software versions on both devices are the same. If the software version is different, the "Rules could not be pasted because they are not compatible with the version of this device" error appears when you attempt to paste the rules. You can click the **Details** link to know the details.

To copy rules to another FDM-managed device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to copy the rule from.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to copy and click **Copy** in the **Actions** pane on the right.

Step 6 Click **Inventory** and navigate to the FDM-managed device you want to paste the rules to.

Step 7 In the **Management** pane on the right, click **Policy**.

Step 8 In the policy where you want to paste the rule(s) you just copied, select the rule that your copied rule(s) should precede or follow and, in the **Actions** pane, click **Paste Before** or **Paste After**.

Step 9 Select any access control rule you want for pasting the copied rules around it and in the **Actions** pane, click one of the following options:

- **Paste Before** automatically one or more rules above the selected rule, so the copied rules evaluate network traffic before the selected rule.
- **Paste After** automatically one or more rules below the selected rule, so the copied rules evaluate network traffic after the selected rule.

The paste operation can be performed multiple times at any required position.

Note When pasting rules to another FDM-managed device, if a rule with the same name exists, '-Copy' is appended to the original name. If the renamed name also exists, '-Copy n' is appended to the original name. For example, 'rule name-Copy 2'.

Step 10 When you copy rules from one FDM-managed device to another, the **Configuration Status** of the destination device is in 'Not Synced' state. Review your changes and Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device now or wait and deploy multiple changes at once.

Related Information:

- Move FDM-Managed Access Control Rules
- Behavior of Objects when Pasting Rules to Another Device

Move FDM-Managed Access Control Rules

Use this feature to move access control rules by cutting it from their current position in a policy and pasting them to a new position in the same policy or to the policy of a different FDM-managed device. You can paste the rule before or after other rules in a policy, so the rule evaluates that network traffic in its proper order within the policy.

Move Rules within the Device

To move rules within an FDM-managed device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device whose policy it is you want to edit.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to move and click **Cut**in the Actions pane on the right. The selected rules are highlighted in yellow. **Note**: If you want to cancel your selection, select any rule and click **Copy**.

Step 6 In the policy where you want to paste the rule(s) you just cut, select the rule that the cut rule(s) should precede or follow and, in the **Actions** pane, click one of the following options:

- **Paste Before** automatically pastes one or more rules above the selected rule, so the cut rules evaluate network traffic before the selected rule.
- **Paste After** automatically pastes one or more rules below the selected rule, so the cut rules evaluate network traffic after the selected rule.

The paste operation can be performed multiple times at any required position.

Note When pasting rules within an FDM-managed device, if a rule with the same name exists, '- Copy' is appended to the original name. If the renamed name also exists, '- Copy n' is appended to the original name. For example, 'rule name - Copy 2'.

Step 7 Review your changes and Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device now or wait and deploy multiple changes at once.

Move a Rule from One FDM-Managed Device Policy to Another FDM-Managed Device Policy

When moving rules from one FDM-managed device policy to another FDM-managed device policy, objects associated with those rules are copied to the new FDM-managed device as well.

Security Cloud Control validates some conditions when pasting the rules. For more information on those conditions, see Behavior of Objects when Pasting Rules to Another Device.

To move rules to another FDM-managed device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device you want to copy the rule from.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to move and click **Cut** in the **Actions** pane on the right.

Step 6 Click **Inventory** and navigate to the FDM-managed device you want to move one or more selected rules to.

Step 7 In the **Management** pane on the right, click **Policy**.

Step 8 In the policy where you want to paste the rule(s) you just cut, select the rule that your cut rule should precede or follow and, in the **Actions** pane, click **Paste Before** or **Paste After**.

- **Paste Before** automatically one or more rules above the selected rule, so the cut rules evaluate network traffic before the selected rule.
- **Paste After** automatically one or more rules below the selected rule, so the cut rules evaluate network traffic after the selected rule.

The paste operation can be performed multiple times at any required position.

Note When pasting rules within an FDM-managed device, if a rule with the same name exists, '-Copy' is appended to the original name. If the renamed name also exists, '- Copy n' is appended to the original name. For example, 'rule name - Copy 2'.

Step 9 When you copy rules from one FDM-managed device to another, the **Configuration Status** of source and destination devices are in 'Not Synced' state. Review your changes and Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device now or wait and deploy multiple changes at once.

Related Information:

- Copy FDM-Managed Access Control Rules
- Behavior of Objects when Pasting Rules to Another Device

Behavior of Objects when Pasting Rules to Another Device

If the rules you cut or copied contain objects, and you paste those rules into another FDM-managed device policy, Security Cloud Control copies the objects in those rules to the destination FDM-managed device when any of the following conditions are met:

For all types of objects (except security zone)

- The destination device does not contain the object; in that case, Security Cloud Control creates the object in the destination device first and then pastes the rule.
- The destination device contains the object with the same name and the same values as the source device.

For security zone objects

- The destination device contains the security zone object with the same name and the same interfaces as the source.
- The destination device does not contain the same security zone object and has interfaces for use on the destination.
- The destination device contains the security zone object, which is empty and has interfaces for use on the destination.

For objects with Active Directory (AD) realm

- Security Cloud Control pastes the rule with Active Directory (AD) realm objects only if the realm with the same name already present on the target device.

Important The paste operation fails in the following conditions:

- If there are differences in the vulnerability, geolocation, intrusion, or URL databases between the two device versions, Security Cloud Control cannot paste the rules into the target device. You need to recreate the rules manually in the new device.
- If the rule you are adding has a security zone that contains the interface of type 'management-only'.

Related Information:

- Copy FDM-Managed Access Control Rules
- Move FDM-Managed Access Control Rules

Source and Destination Criteria in an FDM-Managed Access Control Rule

The Source and Destination criteria of an access rule define the security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the protocols and ports used in the traffic. The default is any zone, address, geographical location, protocol, and port.

To modify the source or destination conditions in an access control rule you can edit the rule using the procedure in Configure the FDM Access Control Policy. Simple edits may be performed without entering edit mode. From the policy page, you can modify a condition in the rule by selecting the rule and clicking the + button within the source or destination condition column and selecting a new object or element in the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

You can use the following criteria to identify the source and destination to match in the rule.

Source Zones, Destination Zones

The security zone objects that define the interfaces through which the traffic passes. You can define one, both, or neither criteria: any criteria not specified applies to traffic on any interface.

- To match traffic leaving the device from an interface in the zone, add that zone to the Destination Zones.
- To match traffic entering the device from an interface in the zone, add that zone to the Source Zones.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones and egress through one of the destination zones.

Use this criteria when the rule should apply based on where the traffic enters or exits the device. For example, if you want to ensure that all traffic going to inside hosts gets intrusion inspection, you would select your inside zone as the Destination Zones while leaving the source zone empty. To implement intrusion filtering in the rule, the rule action must be Allow, and you must select an intrusion policy in the rule.

Note You cannot mix passive and routed security zones in a single rule. In addition, you can specify passive security zones as source zones only, you cannot specify them as destination zones.

Source Networks, Destination Networks

The network objects or geographical locations that define the network addresses or locations of the traffic.

- To match traffic from an IP address or geographical location, configure the Source Networks.
- To match traffic to an IP address or geographical location, configure the Destination Networks.
- If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from the following tabs:

- Network—Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control. You can use objects that define the address using the fully-qualified domain name (FQDN); the address is determined through a DNS lookup.
- Geolocation—Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent. Besides selecting geographical location directly in the rule, you can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

Note To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB).

Source Ports, Destination Ports/Protocols

The port objects that define the protocols used in the traffic. For TCP/UDP, this can include ports. For ICMP, it can include codes and types.

- To match traffic from a protocol or port, configure the **Source Ports**. Source ports can be TCP/UDP only.
- To match traffic to a protocol or port, configure the **Destination Ports/Protocols**. If you add only destination ports to a condition, you can add ports that use different transport protocols. ICMP and other non-TCP/UDP specifications are allowed in destination ports only; they are not allowed in source ports.
- To match traffic both originating from specific TCP/UDP ports and destined for specific TCP/UDP ports, configure both. If you add both source and destination ports to a condition, you can only add ports that share a single transport protocol, TCP or UDP. For example, you could target traffic from port TCP/80 to port TCP/8080.

URL Conditions in an FDM-Managed Access Control Rule

The URL conditions of an access control rule defines the URL used in a web request, or the category to which the requested URL belongs. For category matches, you can also specify the relative reputation of sites to allow or block. The default is to allow all URLs.

URL categories and reputations allow you to quickly create URL conditions for access control rules. For example, you could block all Gaming sites, or all high risk Social Networking sites. If a user attempts to browse to any URL with that category and reputation combination, the session is blocked.

Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

To modify the URL and URL Category conditions in an access control rule, you can edit the rule using the procedure in Configure the FDM Access Control Policy. Simple edits may be performed without entering edit mode. From the policy page, you can modify a URL condition in the rule by selecting the rule and clicking the + button within the URL condition column and selecting a new object, element, URL reputation, or URL category from the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

Click the blue plus icon  and select URL objects, groups, or URL categories and click **Save**. You can click Create New Object if the URL object you require does not exist. See Create or Edit an FDM-Managed URL Object for more information about URL objects.

License Requirement for URL Filtering

To use URL filtering, you need to have the **URL** license enabled on your FDM-manageddevice.

Specifying a Reputation for a URL Category Used in a Rule

By default, all URLs in a URL category are treated by a rule the same way. For example, if you have a rule that blocks Social Network URLs, you will block all of them regardless of reputation. You can adjust that setting so that you block only high-risk Social Network sites. Likewise, you could allow all URLs from a URL category except the high-risk sites.

Use this procedure to use a reputation filter on a URL category in an access control rule:

Procedure

Step 1 From the FDM Policy page, select the rule you want to edit.

Step 2 Click **Edit**.

Step 3 Click the **URLs** tab.

Step 4 Click the blue plus button  and select a URL Category.

Step 5 Click **Apply Reputation to Selected Categories** or the **Any Reputation** link on the URL Category you just picked.

Step 6 Uncheck the **Any Reputation** check box.

Step 7 Filter URLs by reputation:

- If the rule has a blocking action, slide the reputation slider to the right to block only the sites with the reputations marked in red. For example, if you slide the slider to "Sites with Security Risks," a blocking rule would block "Sites with Security Risks," "Suspicious Sites," and "High-Risk sites" but it would allow traffic from "Well-known Sites" and "Benign Sites."
- If the rule has an allow action, slide the reputation slider to the right to allow only the sites with the reputations marked in green. For example, if you slide the slider to "Benign Sites," the rule will allow

traffic from "Well-Known Sites" and "Benign Sites" but not allow traffic from "Sites with Security Risks," "Suspicious Sites," and "High-Risk sites."

Step 8 Click **Save**.

Step 9 Click **Select**.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Intrusion Policy Settings in an FDM-Managed Access Control Rule

Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings.

License and Action Requirements for Intrusion Policies

- **Licenses**-To add intrusion policies to a rule, you need to enable an license on the FDM-managed device
- **Rule action**-you can configure intrusion and file policies on rules that **allow** traffic only. Inspection is not performed on rules set to **trust** or **block** traffic. In addition, if the default action for the access control policy is **allow**, you can configure an intrusion policy but not a file policy.

Available Intrusion Policies for an Access Control Rule

For access control rules that allow traffic, you can select one of the following intrusion policies to inspect traffic for intrusions and exploits. An intrusion policy examines decoded packets for attacks based on patterns, and can block or alter malicious traffic.

The policies are listed from least to most secure:

- **Connectivity over Security**—This policy is built for organizations where connectivity (being able to get to all resources) takes precedence over network infrastructure security. The intrusion policy enables far fewer rules than those enabled in the Security over Connectivity policy. Only the most critical rules that block traffic are enabled. Select this policy if you want to apply some intrusion protection but you are fairly confident in the security of your network.
- **Balanced Security and Connectivity**—This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.
- **Security over Connectivity**—This policy is built for organizations where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic. Select this policy when security is paramount or for traffic that is high risk.
- **Maximum Detection**—This policy is built for organizations where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policy, with the potential for even greater operational impact. For example, the intrusion policy enables rules in a large number of threat categories including malware, exploit kit, old and common vulnerabilities, and known in-the-wild exploits. If you select this policy, carefully evaluate whether too much legitimate traffic is being dropped.

Related Information

- Intrusion, File, and Malware Inspection in FDM-Managed Access Control Policies

File Policy Settings in an FDM-Managed Access Control Rule

Use file policies to detect malicious software, or *malware*, using Advanced Malware Protection for Firepower (AMP for Firepower). You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware.

AMP for Firepower uses the AMP cloud to retrieve dispositions for possible malware detected in network traffic, and to obtain local malware analysis and file pre-classification updates. The management interface must have a path to the Internet to reach the AMP cloud and perform malware lookups. When the device detects an eligible file, it uses the file's SHA-256 hash value to query the AMP cloud for the file's disposition. The possible dispositions are:

- Malware—The AMP cloud categorized the file as malware. An archive file (e.g. a zip file) is marked as malware if any file within it is malware.
- Clean—The AMP cloud categorized the file as clean, containing no malware. An archive file is marked as clean if all files within it are clean.
- Unknown—The AMP cloud has not assigned a disposition to the file yet. An archive file is marked as unknown if any file within it is unknown.
- Unavailable—The system could not query the AMP cloud to determine the file's disposition. You may see a small percentage of events with this disposition; this is expected behavior. If you see a number of "unavailable" events in succession, ensure that the Internet connection for the management address is functioning correctly.

License and Action Requirements for File Policies

Licenses-To add file policies to a rule, you need to enable two licenses on the Firepower Device Manager:

- license
- Malware license

Rule action-You can configure file policies on rules that allow traffic only. Inspection is not performed on rules set to trust or block traffic. In addition, if the default action for the access control policy is allow, you can configure an intrusion policy but not a file policy.

Available File Policies for an Access Control Rule

- **None**—Do not evaluate transmitted files for malware and do no file-specific blocking. Select this option for rules where file transmissions are trusted or where they are unlikely (or impossible), or for rules where you are confident your application or URL filtering adequately protects your network.
- **Block Malware All**—Query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.
- **Cloud Lookup All**—Query the AMP cloud to obtain and log the disposition of files traversing your network while still allowing their transmission.

- **Block Office Document and PDF Upload, Block Malware Others**—Block users from uploading Microsoft Office documents and PDFs. Additionally, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.
- **Block Office Documents Upload, Block Malware Others**—Block users from uploading Microsoft Office documents. Additionally, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

Releated Information:

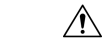
- Intrusion Policy Settings in an FDM-Managed Access Control Rule

Logging Settings in an FDM-Managed Access Control Rule

Logging Settings for Access Control Rule

The logging settings for an access rule determine whether connection events are issued for traffic that matches the rule.

You should log connections according to the security and compliance needs of your organization. If your goal is to limit the number of events you generate and improve performance, only enable logging for the connections critical to your analysis. However, if you want a broad view of your network traffic for profiling purposes, you can enable logging for additional connections.



Caution Logging blocked TCP connections during a Denial of Service (DoS) attack can affect system performance and overwhelm the database with multiple similar events. Before you enable logging for a Block rule, consider whether the rule is for an Internet-facing interface or other interface vulnerable to DoS attack.

Procedure

Procedure

Step 1 Configure the FDM Access Control Policy and click the **Logging** tab.

Step 2 Specify the log action:

- **Log at Beginning and End of Connection**—Issue events at the start and end of a connection. Because end-of-connection events contain everything that start-of-connection events contain, plus all of the information that could be gleaned during the connection, Cisco recommends that you do not select this option for traffic that you are allowing. Logging both events can impact system performance. However, this is the only option allowed for blocked traffic.
- **Log at End of Connection**—Select this option if you want to enable connection logging at the end of the connection, which is recommended for allowed or trusted traffic.
- **Log None**—Select this option to disable logging for the rule. This is the default.

Note When an intrusion policy, invoked by an access control rule, detects an intrusion and generates an intrusion event, the system automatically logs the end of the connection where the intrusion occurred, regardless of the logging configuration of the rule. For connections where an intrusion was blocked, the action for the connection in the connection log is **Block**, with a reason of **Intrusion Block**, even though to perform intrusion inspection you must use an Allow rule.

Step 3 Specify where to send connection events:

If you want to send a copy of the events to an external syslog server, select the server object that defines the syslog server. If the required object does not already exist, you will need to create one. See Create and Edit Syslog Server Objects for more information.

Because event storage on the device is limited, sending events to an external syslog server can provide more long-term storage and enhance your event analysis.

For Secure Logging Analytics for FDM-Managed Devices subscribers:

- If you send events to the Cisco cloud through a Secure Event Connector (SEC), Create a Syslog Server Object for Secure Logging Analytics (SaaS). You will then be able to see these events alongside file policy and malware policy connection events.
- If you send events directly to the Cisco cloud without an SEC, specify when to log events (at the beginning or end of the connection) but do not specify the SEC as the syslog server.

Step 4 File Events

Check **Log Files** if you want to enable logging of prohibited files or malware events. You must select a file policy in the rule to configure this option. The option is enabled by default if you select a file policy for the rule. We recommend you leave this option enabled.

When the system detects a prohibited file, it automatically logs one of the following types of event to the FDM-manageds internal buffer.

- File events, which represent detected or blocked files, including malware files.
- Malware events, which represent detected or blocked malware files only.
- Retrospective malware events, which are generated when the malware disposition for a previously detected file changes.

For connections where a file was blocked, the action for the connection in the connection log is Block even though to perform file and malware inspection you must use an Allow rule. The connection's Reason is either File Monitor (a file type or malware was detected), or Malware Block or File Block (a file was blocked)

Step 5 Click **Save**.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Security Group Tags

About Security Group Tags

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria. Thus, you can block or allow access based on security group membership rather than IP addresses.

In ISE, you can create a SGT and assign host or network IP addresses to each tag. If you assign an SGT to a user's account, the SGT is assigned to the user's traffic. After you configure FDM-managed device to connect to an ISE server and create the SGT, you can create SGT groups in Security Cloud Control and build access control rules around them. Note that you must configure ISE's SGT Exchange Protocol (SXP) mapping before you can associate an SGT to an FDM-managed device. See **Security Group Tag Exchange Protocol** in the Cisco Identity Services Engine Administrator Guide of the version you are currently running for more information.

When an FDM-managed device evaluates SGT as a traffic matching criteria for an access control rule, it uses the following priority:

1. The source SGT defined in the packet, if any. No destination matching is done using this technique. For the SGT to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
2. The SGT assigned to the user session, as downloaded from the ISE session directory. You need to enable the option to listen to session directory information for this kind of SGT matching, but this option is on by default when you first create the ISE identity source. The SGT can be matched to source or destination. Although not required, you would also normally set up a passive authentication identity rule, using the ISE identity source along with an AD realm, to collect user identity information.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is within the range for an SGT, then the traffic matches the access control rule that uses the SGT. The SGT can be matched to source or destination.

Note You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on a relevant collections of tags if that is appropriate.

Version Support

Security Cloud Control currently supports SGT and SGT groups on FDM-managed devices running Version 6.5 and later. an FDM-managed device allows you to configure and connect to an ISE server in Version 6.5 and later but not does not support SGT configuration in the UI until Version 6.7.

From the FDM-managed UI, this means that an FDM-managed device running Version 6.5 or later can download SXP mappings of SGTs but cannot be manually added to objects or access control rules. To make changes to the SGTs for devices running Version 6.5 or Version 6.6, you must use the ISE UI. If the device running Version 6.5 is onboarded to Security Cloud Control, however, you can see the current SGTs associated with the device and create SGT groups.

SGT in Security Cloud Control

Security Group Tags

SGTs are read-only in Security Cloud Control. You cannot create or edit an SGT in Security Cloud Control. To create an SGT, see the Cisco Identity Services Engine Administrator Guide of the version your are currently running.

SGT Groups

Note An FDM-managed device refers to groups of SGTs as SGT dynamic objects. In Security Cloud Control, these lists of tags are currently called SGT groups. You can create an SGT group in Security Cloud Control without referring to the FDM-managed device or ISE UI.

Use SGT groups to identify source or destination addresses based on an SGT assigned by ISE. You can then use the objects in access control rules for purposes of defining traffic matching criteria. You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information.

Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

In order to create an SGT group in Security Cloud Control, you must have at least one SGT already configured and SGT mappings from an ISE server configured for the FDM-managed console of the device you want to use. Note that if more than one FDM-managed device is associated with the same ISE server, an SGT or SGT group can be applied to more than one device. If a device is not associated with an ISE server, you cannot include SGT objects in your access control rule, or apply an SGT group to that device configuration.

SGT Groups in Rules

SGT groups can be added to access control rules; they appear as source or destination network objects. For more information about how networks work in rules, see Source and Destination Criteria in an FDM-Managed Access Control Rule.

You can create an SGT group from the Objects page. See Create an SGT Group, on page 154 for more information.

Create an SGT Group

To create an SGT group that can be used for an access control rule, use the following procedure:

Before you begin

You must have the following configurations or environments configured prior to creating a security group tag (SGT) group:

- FDM-managed device must be running at least Version 6.5.
- You must configure the ISE identity source to subscribe to SXP mappings and enable deploy changes. To manage SXP mappings, see **Configure Security Groups and SXP Publishing in ISE** of the Firepower Device Manager Configuration Guide for the version you're using, Version 6.7 and later.

- All SGTs must be created in ISE. To create an SGT, see the Cisco Identity Services Engine Configuration Guide of the version your are currently running.

Procedure

Step 1 On the left pane, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD > Network**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Click **SGT** and use the drop-down menu to check all the applicable SGTs you want included in the group. You can sort the list by SGT name.

Step 7 Click **Save**.

Note You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Edit an SGT Group

To edit an SGT group, use the following procedure:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Locate the SGT group you want to edit by using object filters and search field.

Step 3 Select the SGT group and click the edit icon  in the **Actions** pane.

Step 4 Modify the SGT group. Edit the name, description, or the SGTs associated with the group.

Step 5 Click **Save**.

Note You cannot create or edit SGTs in Security Cloud Control, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Add an SGT Group to an Access Control Rule

To add an SGT group to an access control rule, use the following procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to add the SGT group to.

Step 4 In the**Management** pane, select **Policy**.

Step 5 Click the blue plus button  for either the **Source** or **Destination** objects and select **SGT Groups**.

Step 6 Locate the SGT group(s) you want to edit by using object filters and search field.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices.

Note If you need to create an additional SGT group, click **Create New Object**. Fill in the required information mentioned in Create an SGT Group and **Add** the SGT group to the rule.

Application Criteria in an FDM-Managed Access Control Rule

The Application criteria of an access rule defines the application used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application.

Although you can specify individual applications in the rule, application filters simplify policy creation and administration. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

In addition, Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

You can specify applications and filters directly in the rule, or create application filter objects that define those characteristics. The specifications are equivalent, although using objects can make it easier to stay within the 50-items-per-criteria system limit if you are creating a complex rule. See Create and Edit a Firepower Application Filter Object for more information about creating an application filter object.

To modify the application and application filters used in a rule, you can edit the rule using the procedure in FDM-Managed Access Control Policy. Simple edits may be performed without entering edit mode. From the policy page, you can modify an application condition in the rule by selecting the rule and clicking the + button within the application condition column and selecting a new object or element in the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

Intrusion, File, and Malware Inspection in FDM-Managed Access Control Policies

Intrusion and file policies work together as the last line of defense before traffic is allowed to its destination:

- Intrusion policies govern the system's intrusion prevention capabilities.
- File policies govern the system's file control and AMP for Firepower capabilities.

All other traffic handling occurs before network traffic is examined for intrusions, prohibited files, and malware. By associating an intrusion or file policy with an access control rule, you are telling the system that before it passes traffic that matches the access control rule's conditions, you first want to inspect the traffic with an intrusion policy, a file policy, or both.

You can configure intrusion and file policies on rules that allow traffic only. Inspection is not performed on rules set to trust or block traffic. In addition, if the default action for the access control policy is allow, you can configure an intrusion policy but not a file policy.

For any single connection handled by an access control rule, file inspection occurs before intrusion inspection. That is, the system does not inspect files blocked by a file policy for intrusions. Within file inspection, simple blocking by type takes precedence over malware inspection and blocking. Until a file is detected and blocked in a session, packets from the session may be subject to intrusion inspection.

Note By default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured. Inspection works with unencrypted traffic only.

Related Information:

- Intrusion Policy Settings in an FDM-Managed Access Control Rule
- File Policy Settings in an FDM-Managed Access Control Rule

Custom IPS Policy in an FDM-Managed Access Control Rule

You cannot have more than one instance of the same custom IPS policy associated to a single device.

Note Associating an IPS policy with an access control rule means that passing traffic is submitted to deep packet inspection. The only supported rule action for an access control rule with an IPS policy is **Allow**.

Use the following procedure to associate a custom IPS policy to an FDM-managed device:

Procedure

Step 1 Create a custom IPS policy. See Configure Firepower Custom IPS Policies for more information.

Step 2 In the left pane, click **Policies** > **FDM** > **Policies**.

Step 3 Scroll or filter through the list of FDM-managed device policies and select the policy you want to associate with a custom IPS policy.

Step 4 Click the blue plus button .

Step 5 In the **Order** field, select the position for the rule within the policy. Network traffic is evaluated against the list of rules in numerical order, 1 to "last."

Step 6 Enter the rule name. You can use alphanumeric characters, spaces, and these special characters: + . _ -

Step 7 Select the **Intrusion Policy** tab. Expand the drop-down menu to see all the available intrusion policies and select the desired custom IPS policy.

Step 8 Define the traffic matching criteria by using any combination of attributes in the remaining tabs: **Source/Destination**, **URLs**, **Applications**, and **File Policy**.

Step 9 (Optional) Click the logging tab to enable logging and collect **connection events** reported by the access control rule.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

TLS Server Identity Discovery in Firepower Threat Defense

You can now perform improved URL filtering and application control on traffic with threat defense's unique TLS Server Identity Discovery that allows control and precision when it comes to your environment. You do not have decrypt the traffic for this feature to work.

Note Support for the Server Identity Discovery feature is limited to Version 6.7 and later.

Enable the TLS Server Identity Discovery

Use the following procedure to enable, or disable, the TLS Server Identity Discovery feature for your FDM-managed access control policies:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device.

Step 4 In the **Management** pane located to the right, select **Policy**.

Step 5 Click the Access Policy Settings gear icon in the upper right corner of the table .

Step 6 Slide the toggle to enable TLS Server Identity Discovery.

Step 7 Click **Save**.

Intrusion Prevention System

The Cisco Talos Intelligence Group (Talos) detects and correlates threats in real time and maintains a reputation disposition on billions of files. The Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that mitigates attacks on your network by using the threat intelligence data from Talos to accurately identify, classify, and drop malicious traffic in real time.

Security Cloud Control provides the ability to activate and tune the IPS feature on FDM-managed devices that run software versions 6.4.x.x through 6.6.0.x and 6.6.1.x.

Note Security Cloud Control currently does not support IPS rule tuning on version 6.7.

On the Security Cloud Control menu bar, navigate **Policies > Signature Overrides** to perform these tasks:

- Resolve inconsistencies in overrides across multiple devices.
- View and hide threat events.
- Override how a threat event is handled by changing the rule action.

Related Information:

- Firepower Intrusion Policy Signature Overrides
- Threat Events
- Troubleshoot Intrusion Prevention System

Threat Events

A threat event report is a report of traffic that has been dropped, or that has generated an alert, after matching one of Cisco Talos' intrusion policies. In most cases, there's no need to tune IPS rules. If necessary, you have the option to override how an event is handled by changing the matching rule action in Security Cloud Control.

Note the following behaviors of the Threats page:

- Threat events that are displayed are not live. Devices are polled hourly for additional Threat events.
- Threat events that are not included in the Viewing Live Events view are not part of Cisco Security Analytics and Logging.
- To see Threat events that you've hidden from view, click the filter icon and check the **view hidden** option.
- If you are a subscriber to Secure Logging Analytics for FDM-Managed Devices , the events you see in Threat Events table do not contain events sent to the Secure Event Connector.

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Firewall Threat Defense** > **Threats Dashboard (FDM)**. You can Object Filters what events are shown and search by source IP address.

Step 2 Click on a threat event to expand the details panel on the right.

a) For more information on the rule, click the **Rule Document** URL in the **Rule Details** section.

b) To hide this event, check the toggle switch for **Hide Events**. The event handling continues as is, but you won't see it here, unless you click **View Hidden** or un-hide this event.

c) To edit rule overrides, click **Tune Rule**. When you change a rule action in Security Cloud Control, the override applies to all the pre-defined policies. This is different than in the FDM-managed device where each rule can be different from policy to policy.

Note Security Cloud Control provides the ability to tune rules on FDM-managed devices that run software versions 6.4.x.x through 6.6.0.x and 6.6.1.x. Security Cloud Control currently does not support rule tuning on FDM-managed Version 6.7.

- In the **Override All** devices pull-down, select an action and click **Save**.
  - **Drop**-This choice creates an event when this rule matches traffic and then drops the connection. Use this action to tighten security of certain rules. For example, specifying Drop would make security stricter when the Talos rule is matched even if the "Connectivity over Security" policy is specified for the access control rule.
  - **Alert**-This choice creates an event when this rule matches traffic, but it does not drop the connection. A use case for "Alert" is when traffic is blocked, but the customer wants to allow, it and look at the alerts before disabling the rule.
  - **Disabled**-This choice prevents traffic from being matched to the rule. No events are generated. The use case for "Disabled" is to stop false positives in reports, or remove rules that do not apply to your environment, like disabling Apache httpd rules if you don't use httpd.
  - **Default**-This choice returns a rule to the default action it was assigned by Talos, for the intrusion policy it is listed in. For example, when you return an intrusion rule to "Default" that may mean its action returns to "Alert" in the "Connectivity over Security" policy and "Block" in the "Balanced Security and Connectivity" policy.
- To edit rule overrides by device, check the **Advanced Options** slider. This section shows you the configured rule action for each device, which you can change by checking the affected device, selecting an override action, and clicking **Save**.
- **Affected Devices** does not indicate the source devices. Instead, it shows the FDM-managed devices reporting the event.

Note

- Click the refresh ( ) button to refresh the table that shows threats based on the current search filters.
- Click the export ( ) button to download the current summary of the threats to a comma-separated value (.csv) file. You can open the .csv file in a spreadsheet application such as Microsoft Excel to sort and filter the items on your list. Security Cloud Control exports the basic threat details to the file except for additional information such as time, source, and device.

Step 3 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Firepower Intrusion Policy Signature Overrides

In most cases, there's no need to tune any IPS rules. If necessary, you have the option to override how an event is handled by changing the matching rule action in Security Cloud Control. Security Cloud Control gives you options to resolve issues with the overrides.

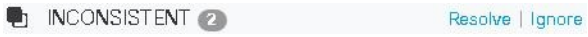
Manage Signature Overrides

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Signature Overrides**. You can Object Filterswhat devices and policy override policies are shown. You can also search for intrusion policies by name or intrusion rule SID.

Step 2 Click on the name of policy override policy to expand the details panel on the right.

Step 3 In the **Issues** pane, a badge indicates the overrides are inconsistent across the devices. You can see the INCONSISTENT field with the number of devices affected:



a) **To ignore the issue**, click **Ignore**. This doesn't change the issue but removes the indicator badge from the **Issues** column.

b) **To resolve the issue**, click **Resolve**. In the left panel, select the policies to compare and show their consistent and inconsistent overrides.

- To merge the policies together:
  1. Click **Resolve by Merging** to combine them into a single policy with the same overrides on all its devices.
  2. Click **Confirm**.
- To rename a policy:
  1. In the policy's section, click **Rename** and give it a different name.
  2. Click **Confirm**.
- To ignore a policy:
  1. In the policy's section, click **Ignore**.
  2. Click **Confirm**.
- To ignore all the inconsistencies, click **Ignore All**.

Step 4 If there are individual Talos intrusion rules that were changed on the device using an FDM-managed device you will see them in the **Overrides** pane. You can change the override action for an intrusion rule by clicking **Tune** link and choosing an override action. This action will be applied to that rule in all of the Talos intrusion policies it's used in. Note that if you choose to restore the default action rule (**Default**), you cannot tune the intrusion rule again until it is triggered by the environment.

- Connectivity over Security
- Balanced Security and Connectivity
- Security over Connectivity
- Maximum Detection

For consistency across devices, the override action will be saved to every device associated with the intrusion override policy.

These are the effects of the override action:

- **Drop**-This choice creates an event when this rule matches traffic and then drops the connection. Use this action to tighten security of certain rules. For example, specifying Drop would make security stricter when the Talos rule is matched even if the "Connectivity over Security" policy is specified for the access control rule.
- **Alert**-This choice creates an event when this rule matches traffic, but it does not drop the connection. A use case for "Alert" is when traffic is blocked, but the customer wants to allow, it and look at the alerts before disabling the rule.
- **Disabled**-This choice prevents traffic from being matched to the rule. No events are generated. The use case for "Disabled" is to stop false positives in reports, or remove rules that do not apply to your environment, like disabling Apache httpd rules if you don't use httpd.
- **Default**-This choice is only applicable if the rule's default action is different in the Talos intrusion policy levels. For example, when you return an intrusion rule to "Default" that may mean its action returns to "Alert" in the "Connectivity over Security" policy and "Block" in the "Balanced Security and Connectivity" policy.
- Edit rule overrides with the following options:
  - **Override for all devices** - This option sets the required action to all the devices managed by Security Cloud Control. Select an option from the drop-down menu. If the rule has different override values for different intrusion override policies, the drop-down option is "Multiple" by default.
  - **Edit rule overrides by device** - check the **Advanced Options** slider and select the **Overrides by Devices** tab. This option shows you the configured rule action for each device, which you can change by checking the affected device, selecting an override action, and clicking **Save**.
  - **Edit rule overrides by policy** - check the **Advanced Options** slider and select the **All Overrides** tab. This section is only applicable if your tenant has more than one IPS policy configured. You can manage all IPs policies from this page, including policies that have more than one device associated to it.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create A Signature Override

You can only create signature overrides for IPS rules that are already triggered on an FDM-managed device. When you create a signature override in Security Cloud Control, the override is automatically applies the configured action (**Drop**, **Alert**, **Disabled**, **Default**) to all of the policy levels.

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Firewall Threat Defense** > **Threats Dashboard (FDM)**.

Step 2 Select a threat from the table and expand it. In the Tune Actions pane, click **Tune**.

Step 3 Tune the rules as described in **step 4** in the Firepower Intrusion Policy Signature Overrides procedure.

Step 4 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Remove A Signature Override

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Signature Overrides**.

Step 2 Click on the name of override to expand the details panel on the right.

Step 3 Expand the Overrides pane and select the override you want to remove, then click **Tune**.

Step 4 Set the default action to **Default**.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Custom Firepower Intrusion Prevention System Policy

About Custom IPS Policies

With the introduction of version 6.7, the improved Snort 3 processing engine allows you to create and customize Intrusion Prevention System (IPS) policies using rules provided by the Cisco Talos Intelligence Group (Talos). The best practice is to create your own policy based on the provided Talos policy templates and change that if you need to adjust rule actions.

Note At this time, Security Cloud Control does not support custom IPS rules. You can create and modify custom IPS policies with rules that are provided by Talos, but you cannot create your own IPS rules and apply them to custom IPS policies.

The base templates include the same list of intrusion rules (also known as signatures), but they differ in the actions taken for each rule. For example, a rule might be enabled in one policy, but disabled in another policy.For another example, you may find that a particular rule is giving you too many false positives, where the rule is blocking traffic that you do not want blocked; you can disable the rule without needing to switch to a less-secure intrusion policy. You could alternatively change it to alert on matches without dropping traffic.

IPS Policy Base Template

The base templates include the same list of intrusion rules (also known as signatures), but they differ in the actions taken for each rule. For example, a rule might be enabled in one policy, but disabled in another policy. For another example, you may find that a particular rule is giving you too many false positives, where the rule is blocking traffic that you do not want blocked; you can disable the rule without needing to switch to a less-secure intrusion policy. You could alternatively change it to alert on matches without dropping traffic.

The base templates provided are suggested configurations based on the type of protection your network might need. You can use any of the following templates as the base when you create a new policy:

Caution Do **not** modify the default IPS policies provided with an FDM-managed device enabled with Snort 3. We **strongly** recommend creating new custom IPS policies based on the templates below, and to use a unique name for the new policy that is different from the names of the default IPS policies listed below. If you need to troubleshoot your policies, Cisco TAC can easily locate the custom policy and revert to a default policy; this keeps your network protected without losing your customized changes.

The base templates provided are suggested configurations based on the type of protection your network might need. You can use any of the following templates as the base when you create a new policy:

- **Maximum Detection** - These policies are built for networks where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact.
- **Security Over Connectivity** - These policies are built for networks where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.
- **Balanced Security and Connectivity** - These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types.
- **Connectivity Over Security** - These policies are built for networks where connectivity, the ability to get to all resources, takes precedence over network infrastructure security. Only the most critical rules that block traffic are enabled.
- **No Rules Active** - The rules included in the policy are disabled by default.

Tip The **Maximum Detection** base template requires a considerable amount of memory and CPU to work effectively. Security Cloud Control recommends deploying IPS policies using this template to models such as the 2100, 4100, or virtual device.

As new vulnerabilities become known, Talos releases intrusion rule updates. These rule updates can modify any Cisco-provided network analysis or intrusion policy, and may provide new and updated intrusion rules and preprocessor rules that are automatically applies to existing rules and policy settings. Rule updates might also delete rules from the existing template bases and provide new rule categories, as well as modify the default variable set.

IPS Policy Mode

By default, all intrusion policies operate in **Prevention** mode to implement an IPS. In the Prevention inspection mode, if a connection matches an intrusion rule whose action is to drop traffic, the connection is actively blocked.

If you instead want to test the effect of the intrusion policy on your network, you can change the mode to **Detection**, which implements an Intrusion Detection System (IDS). In this inspection mode, drop rules are treat like alert rules, where you are notified of matching connections, but the action result becomes **Would Have Blocked**, and connections are never in fact blocked.

IPS Rule Group Security Level

Security Cloud Control allows you to modify the security level of the rule groups included in your policy. Note that this security level is applied to all the rules in the rule group and not to individual rules.

Note Changes made a rule group's security level are automatically submitted and cannot be reverted. You do not have to click **Save** to submit security level modifications. You must manually change the security level back.

IPS Rule Action

Modify the actions of an individual rule or multiple rules within a rule group at any time. IPS rules can be set as the following options:

- **Disabled**—Do not match traffic against this rule. No events are generated.
- **Alert**—Create an event when this rule matches traffic, but do not drop the connection.
- **Drop**—Create an event when this rule matches traffic, and also drop the connection.

FDM Templates and Custom IPS Policy

Templates derived from a device with Snort 3 enabled can only be applied to devices that also have Snort 3 enabled. Due to the variability in rules supported and processed by Snort 2 and Snort 3, a template configured with Snort 3 cannot fully support and protect a device configured with Snort 2. See Upgrade to Snort 3.0 for more information.

If you happen to use the ASA Migration tool to create an FDM template from an ASA configuration, we **strongly** recommend not configuring, or un-configuring any IPS policies. ASA devices do not support the Snort engine and migrating IPS policies from an ASA configuration to an FDM-managed device configuration may cause issues. If you do use the ASA migration tool, we recommend creating custom IPS policies for the device after creating and deploying the template.

See FDM-Managed Device Templates for more information about templates.

Rulesets and Custom IPS Policy

Rulesets are not yet support on devices configured for Snort 3. The following limitations apply:

- You cannot attach rulesets to Snort 3-enabled devices.
- You cannot create a ruleset from an existing device that has Snort 3 installed.
- You cannot associate a custom IPS policy to a ruleset.

Prerequisites

You can view the available IPS policies from the **Intrusion policies** page, but you cannot create or modify custom IPS policies without the following prerequisites:

Device Support

- Firepower 1000 series
- Firepower 2100 series

- Firepower 4100 series
- Threat Defense virtual with AWS
- Threat Defense virtual with Azure

Software Support

s

Devices **must** be running at least version 6.7 and Snort 3.

If your device is running a version prior to 6.7, upgrade your device. See Upgrade a Single FDM-Managed Device for more information.

If your device is running version 6.7 with Snort 2, please note that some intrusion rules in Snort 2.0 might not exist in Snort 3.0. See Upgrade to Snort 3.0 for more information.

Note To find out what version of software version and Snort engine your device is running, simply locate and select the device on the **Inventory** page and look at the **Device Details**

Related Information:

- Configure Firepower Custom IPS Policies
- Custom IPS Policy in an FDM-Managed Access Control Rule

Configure Firepower Custom IPS Policies

Before you create or modify a custom IPS policy for your FDM-managed device in Security Cloud Control, be sure to read the Custom Firepower Intrusion Prevention System Policy.

At this time, Security Cloud Control does **not** support custom IPS rules. You can create and modify custom IPS policies with rules that are provided by Talos, but you cannot create your own IPS rules and apply them to custom IPS policies.

If you experience issues creating or editing IPS policies in Security Cloud Control, see Troubleshoot Intrusion Prevention System, on page 718 for more information.

Note You cannot delete or reorder the rules within a custom IPS policy's rule group.

Create a Custom IPS Policy

Use the following procedure to create a new custom IPS policy with the IPS rules provided by Talos:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Intrusion Prevention**.

Step 2 Click the blue plus button  .

Step 3 Expand the drop-down menu of the **Base Template**. If your device is running version 7.2 with Snort 3, you must expand the drop-down and then click **Choose** to select the template.If the device is running version 7.1.x and earlier, simply expand the drop-down menu and select one of the following templates:

- **Maximum Detection** - These policies are built for networks where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact.

  Tip The **Maximum Detection** base template requires a considerable amount of memory and CPU to work effectively. Security Cloud Control recommends deploying IPS policies using this template to models such as the 2100, 3100, 4100, or threat defense virtual.

- **Security Over Connectivity** - These policies are built for networks where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.
- **Balanced Security and Connectivity** - These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types.
- **Connectivity Over Security** - These policies are built for networks where connectivity, the ability to get to all resources, takes precedence over network infrastructure security. Only the most critical rules that block traffic are enabled.
- **No Rules Active** - The rules included in the policy are disabled by default.

Step 4 Enter a **Name** for the policy.

We **strongly** recommend using a name that is unique and different from the default base templates. If you ever need to troubleshoot your IPS policy, Cisco TAC can easily locate the custom policy and revert to a default policy; this keeps your network protected without losing your customized changes.

Step 5 (Optional) Enter a **Description** for the policy.

Step 6 Select the **IPS Mode**:

- **Prevention** - If a connection matches an intrusion rule whose action is to drop traffic, the connection is actively blocked.
- **Detection** - If a connection matches an intrusion rule whose action is to drop traffic, the action result becomes **Would Have Blocked** and no action is taken.

Step 7 Click **Save**.

What's Next?

Add your IPS policy to an FDM-managed device access control rule. See Custom IPS Policy in an FDM-Managed Access Control Rule for more information.

Edit a Custom IPS Policy

You can edit an existing IPS policy if you have onboarded an FDM-managed device that already has an IPS policy, if you created an IPS policy in FDM and Security Cloud Control reads the policy from the deployed configuration, or if you just created a new IPS policy.

Use the following procedure to modify an existing custom IPS policy:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Intrusion Prevention**.

Step 2 Identify the IPS policy you want to edit. Click **Edit**.

Step 3 At the top of the page, click the edit icon .

Step 4 Edit the following desired fields:

- Base Template.
- Name.
- Description.
- IPS Mode.

Step 5 Click **Save**.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit Rule Groups in a Custom IPS Policy

You can override the default action of a rule within a rule group. Use the following procedure to edit the rules contained within the rule group

Procedure

Step 1

Step 2 In the left pane, click **Policies** > **FDM** > **Intrusion Prevention**.

Step 3 Identify the IPS policy you want to edit. Click **Edit**.

Step 4 From the Rule Group tab located to the left, expand the desired rule group. From the expanded list, select the group.

Step 5 Edit the rule group:

a) Edit the **Security Level** of the entire rule group by selecting the security level bar. Manually drag the security level to the type of security you want applied to the entire rule group. Click **Submit**

b) Edit the **Rule Action** of an individual rule by expanding the rule's drop-down menu located to the right.

c) Edit the **Rule Action** of multiple rules by selecting the checkboxes of the desired rules and expanding the drop-down menu located above the table of rules. This selection impacts all selected rules.

d) Edit the **Rule Action** of all the rules by selecting the checkbox in the title row of the table and expanding the drop-down menu located above the table of rules. This selection impacts all the rules in the rule group.

Step 6 Click **Save** at the top of the policy page.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Delete a Custom IPS policy

Use the following procedure to delete a custom IPS policy from Security Cloud Control:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Intrusion Prevention**.

Step 2 Identify the IPS policy you want to edit. Click **Delete**.

Step 3 Click **OK** to delete the policy.

Step 4 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Security Intelligence Policy

About Security Intelligence

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. The system drops the traffic on the blocked list before evaluating it with the access control policy, thus reducing the amount of system resources used.

You can block traffic based on the following:

- **Cisco Talos feeds**—Cisco Talos provides access to regularly updated security intelligence feeds. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations. The system downloads feed updates regularly, and thus new threat intelligence is available without requiring you to redeploy the configuration.

Note Cisco Talos feeds are updated by default every hour. You can change the update frequency, and even update the feeds on demand, by logging into Firepower Device Manager and navigating from the home page: Device > Updates > View Configuration.

- **Network and URL objects**—If you know of specific IP addresses or URLs you want to block, you can create objects for them and add them to the Blocked list or the Allowed list.

You create separate blocked and allowed lists for IP addresses (networks) and URLs.

License Requirements for Security Intelligence

You must enable the license on the FDM-managed device to use Security Intelligence.

For more information, see the **Security Intelligence Feed Categories** section of the Security Policies chapter of the appropriate Cisco FTD Configuration Guide for Firepower Device Manager.

Configure the Firepower Security Intelligence Policy

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections are still evaluated by access control policies and might eventually be dropped. You must enable the license to use Security Intelligence.

Configure Firepower Security Intelligence Policy

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the **FTD** tab and select the FDM-managed device for which you are going to create or edit a security intelligence policy.

Step 5 In the **Management** pane at the right, click **Policy.**

Step 6 In the FDM-managed device Policies page, click **Security Intelligence** in the policy bar.

Step 7 If the policy is not enabled, click the Security Intelligence slider to enable it or click **Enable** in the About Security Intelligence information box.

Note You can disable Security Intelligence at any time by clicking the Security Intelligence toggle off. Your configuration is preserved, so that when you enable the policy again you do not need to reconfigure it.

Step 8 Select the row for **Blocked List**. Notice that, depending on your table view, there are plus signs in the networks, network objects, network feeds, URLs, URL objects, and URL feeds columns.

- In the **Add Networks to Blocked List** dialog box and **Add URL Object to Blocked List** dialog box, you can search for an existing object or create one to suit your needs. Check the object you want to block and then click **Select**.

  Note Security Intelligence ignores IP address blocks using a /0 netmask. This includes the any-ipv4 and any-ipv6 network objects. Do not select these objects for network block-listing.

- In the **Add URL Objects to Blocked List** and **Add Network Feeds to Blocked List** dialog, check a feed that you want to block and click **Select**. You can read the description of the feed by clicking the down arrow at the end of the feed row. They are also described in Security Intelligence Feeds for Firepower Security Intelligence Policies.

Step 9 If you know there are networks, IP addresses, or URLs that are included in the any of the network groups, network feeds, URL objects, or URL feeds you specified in the previous step, that you want to make an exception for, click the row for the **Allowed List**.

Step 10 Select or create objects for the networks, IP addresses, and URLs that you want to make exceptions for. When you click **Select** or **Add** they are added to the Allowed List row.

Step 11 (Optional) To log events generated by the Security Intelligence policy:

a) Click the Logging Settings  icon to configure logging. If you enable logging, any matches to blocked list entries are logged. Matches to exception entries are not logged, although you get log messages if exempted connections match access control rules with logging enabled.

b) Enable event logging by clicking the **Connection Events Logging** toggle.

c) Choose where to send your events:

- Clicking **None** saves events to your FDM-managed device. They are visible in the FDM Events viewer. Storage space on the FDM-managed device is very limited. It is best to store your connection events on a syslog server, by defining a syslog server object, instead of choosing None.
- Clicking **Create** or **Choose** allows you to create or choose a syslog server, represented by a syslog server object, to send logging events to. Because event storage on the device is limited, sending events to an external syslog server can provide more long-term storage and enhance your event analysis.

If you have a subscription to Cisco Security Analytics and Logging, send events to a Secure Event Connector by Create a Syslog Server Object for Secure Logging Analytics (SaaS). See Secure Logging Analytics for FDM-Managed Devices for more information about this feature.

Step 12 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Making Exceptions to the Firepower Security Intelligence Policy Blocked Lists

For each blocked list you create in a Configure the Firepower Security Intelligence Policy, you can create an associated allowed list. The only purpose of the allowed list is to make an exception for IP addresses or URLs that appear in the blocked list. That is, if you find an address or URL you need to use, and you know to be safe, is in a feed configured on the blocked list, you can exempt that address or URL by putting in the allowed list. This way, you don't need to remove an entire feed from the blocked list for the sake of one address or URL.

After passing through the security intelligence policy, allowed traffic is subsequently evaluated by the access control policy. The ultimate decision on whether the connections are allowed or dropped is based on the access control rule the connections match. The access rule also determines whether intrusion or malware inspection is applied to the connection.

Security Intelligence Feeds for Firepower Security Intelligence Policies

The following table describes the categories available in the Cisco Talos feeds. These categories can be entered in both the network and URL blocked list.

Category	Description
attackers	Active scanners and block-listed hosts known for outbound malicious activity.
bogon	Bogon networks and unallocated IP addresses.

Category	Description
bots	Sites that host binary malware droppers.
CnC	Sites that host command-and-control servers for botnets.
dga	Malware algorithms used to generate a large number of domain names acting as rendezvous points with their command-and-control servers.
exploitkit	Software kits designed to identify software vulnerabilities in clients.
malware	Sites that host malware binaries or exploit kits.
open_proxy	Open proxies that allow anonymous web browsing.
open_relay	Open mail relays that are known to be used for spam.
phishing	Sites that host phishing pages.
response	IP addresses and URLs that are actively participating in malicious or suspicious activity.
spam	Mail hosts that are known for sending spam.
suspicious	Files that appear to be suspicious and have characteristics that resemble known malware.
tor_exit_node	Tor exit nodes.

FDM-Managed Device Identity Policy

Identity Policy Overview

Use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users and groups, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

For example, you can identify who owns the host targeted by an intrusion event, and who initiated an internal attack or port scan. You can also identify high bandwidth users and users who are accessing undesirable web sites or applications.

You can then view usage based on user identity in the dashboards, and configure access control based on Active Directory (AD) realm object (which matches all users on that AD), special identities (such as failed authentication, guest, no authentication required, or unknown identity), or user groups.

You can obtain user identity using the following methods:

- Passive authentication—For all types of connections, obtain user identity from other authentication services without prompting for username and password.

- Active authentication—For HTTP connections only, prompt for username and password and authenticate against the specified identity source to obtain the user identity for the source IP address.

Establishing User Identity Through Passive Authentication

Passive authentication gathers user identity without prompting the user for username and password. The system obtains the mappings from the identity sources you specify.

You can passively obtain user-to-IP address mappings from the following sources:

- Remote access VPN logins. The following user types are supported for passive identity:
  - User accounts defined in an external authentication server.
  - Local user accounts that are defined in FDM-managed device.
- Cisco Identity Services Engine (ISE); Cisco Identity Services Engine Passive Identity Connector (ISE PIC).

If a given user is identified through more than one source, the remote access VPN login identity takes precedence.

Establishing User Identity through Active Authentication

Authentication is the act of confirming the identity of a user.

With active authentication, when an HTTP traffic flow comes from an IP address for which the system has no user-identity mapping, you can decide whether to authenticate the user who initiated the traffic flow against the directory configured for the system. If the user successfully authenticates, the IP address is considered to have the identity of the authenticated user.

Failure to authenticate does not prevent network access for the user. Your access rules ultimately decide what access to provide these users.

Dealing with Unknown Users

When you use an FDM-managed device to configure the directory server for the identity policy, FDM-managed downloads user and group membership information from the directory server. The Active Directory information is refreshed every 24 hours at midnight or whenever you edit and save the directory configuration (even if you do not make any changes).

If a user succeeds in authenticating when prompted by an active authentication identity rule, but the user's name is not in the downloaded user identity information, the user is marked as Unknown. You will not see the user's ID in identity-related dashboards, nor will the user match group rules.

However, any access control rules for the Unknown user will apply. For example, if you block connections for Unknown users, these users are blocked even though they succeeded in authenticating (meaning that the directory server recognizes the user and the password is valid).

Thus, when you make changes to the directory server, such as adding or deleting users, or changing group membership, these changes are not reflected in policy enforcement until the system downloads the updates from the directory.

If you do not want to wait until the daily midnight update, you can force an update by editing the directory realm information (login to an FDM-managed device and navigate Objects > Identity Sources, then edit the realm). Click **OK**, then deploy changes. The system will immediately download the updates.

Note You can check whether new or deleted user information is on the FDM-managed system by logging in to an FDM-managed device and navigating **Policies** > **Access Control**, clicking the **Add Rule** (+) button, and looking at the list of users on the Users tab. If you cannot find a new user, or you can find a deleted user, then the system has old information

How to Implement an Identity Policy

If you want to manage identity policies for your FDM-managed device using Security Cloud Control you need to create identity sources first. You can configure the remaining settings using Security Cloud Control.

When configured correctly, you will be able to see usernames in the monitoring dashboards and events in FDM. You will also be able to use user identity in access control and SSL decryption rules as a traffic-matching criteria.

Note At this time, Security Cloud Control can not configure some of the components needed to implement identity policies such as remote access VPN and Cisco Identity Services Engine. These components must be configured in FDM, which is the local manager of the device. Some of the steps in the procedure below indicate that you must use FDM to configure some identity components to implement identity policies.

Procedure

The following procedure provides an overview of what you must configure to get identity policies to work:

Procedure

Step 1 Create the AD identity realm. Whether you collect user identity actively or passively, you need to configure the Active Directory (AD) server that has the user identity information. See Create an FTD Active Directory Realm Object for more information.

Step 2 If you want to use passive authentication identity rules, configure the passive identity sources **using FDM**.

You can configure any of the following, based on the services you are implementing in the device and the services available to you in your network.

- Remote access VPN—If you intend to support remote access VPN connections to the device, user logins can provide the identity based on the AD server or on local users (those defined within an FDM-managed device). For information on configuring remote access VPN, see the Configuring Remote Acces VPNs chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version running on your device.
- Cisco Identity Services Engine (ISE) or Cisco Identity Services Engine Passive Identity Connector (ISE PIC)—If you use these products, you can configure the device as a pxGrid subscriber, and obtain user identity from ISE. See the Configure Identity Services Engine chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for instructions.

Step 3 **Using** Security Cloud Control, enable the identity policy and configure passive or active authentication. See Configure Identity Policy Settings for more information.

Step 4 **Using** Security Cloud Control, Configure the Identity Policy Default Action. If your intention is to use passive authentication only, you can set the default action to passive authentication and there is no need to create specific rules.

Step 5 **Using** Security Cloud Control, Configure Identity Rules. Create rules that will collect passive or active user identities from the relevant networks.

Step 6 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Identity Policies

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the FDM dashboards, and configure access control based on user or user group.

The following is an overview of how to configure the elements required to obtain user identity through identity policies:

Procedure

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 Click **Identity** in the Policy bar.

Step 5 If you have not yet enabled an identity policy, read about passive and active authentication and click **Enable**. You are enabling an identity policy, *not* a passive authentication policy or an active authentication policy. The rules in the policy will specify active or passive authentication.

Step 6 Manage the identity policy:

After you configure identity settings, this page lists all rules in order. Rules are matched against traffic from top to bottom with the first match determining the action to apply. You can do the following from this page:

- **To enable or disable the identity policy**, click the identity toggle. See Configure Identity Policy Settings for more information.
- **To read the passive authentication settings**, click the button next to the **Passive Auth** label on the identity bar. See Configure Identity Policy Settings for more information.
- **To enable active authentication,** click the button next to the **Active Auth** label on the identity bar. See Configure Identity Policy Settings for more information.
- **To change the default action**, click the default action button and select the desired action. See Configure the Identity Policy Default Action.
- **To move a rule in the table**, select the rule and click the up or down arrow at the end of the rule's row in the rule table.

- **To move a rule in the table**, select the rule and click the up or down arrow at the end of the rule's row in the rule table.
- **To configure rules**:
  - To create a new rule, click the plus  button.
  - To edit an existing rule, select the rule and click **Edit** in the Actions pane. You can also selectively edit a rule property by clicking on the property in the table.
  - To delete a rule you no longer need, select the rule and click **Remove** in the Actions pane.

For more information on creating and editing identity rules, see Configure Identity Rules.

Step 7 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Identity Policy Settings

For identity policies to work, you must configure the sources that provide user identity information. The settings you must configure differ based on the type of rules you configure: passive, active, or both.

Note At this time, Security Cloud Control can not configure some of the components needed to implement identity policies such as active directory identity realms, remote access VPN, and Cisco Identity Services Engine. These components must be configured in FDM, which is the local manager of the device. Some of the steps in the procedure below indicate that you must use FDM to configure some identity components to implement identity policies.

Procedure

Before you begin

Ensure that time settings are consistent among the directory servers, FDM-managed device, and clients. A time shift among these devices can prevent successful user authentication. "Consistent" means that you can use different time zones, but the time should be the same relative to those zones; for example, 10 AM PST = 1 PM EST.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 **Enable Identity policies** by clicking the Identity toggle. Or, you can click the button, review the descriptions of passive and active authentication and click **Enable** in the dialog.

Step 5 **Read the Passive Authentication** settings. Click the **Passive Auth** button on the identity bar.

The Passive Authentication button shows **Enabled** if you have configured remote access VPN or Cisco Identity Services engine using Firepower Device Manager.

You must have configured at least one passive identity source to create passive authentication rules.

Step 6 **Configure Active Authentication.** When an identity rule requires active authentication for a user, the user is redirected to the captive portal port on the interface through which they are connected and then they are prompted to authenticate.

a) Click the **Active Auth** button on the Identity bar.

b) If you have not already, enable SSL Description by clicking the **Enable** link. If you don't see the Enable link, skip to step "c".

1. From the **Select Decrypt Re-Sign Certificate** menu, select the internal CA certificate to use for rules that implement decryption with re-signed certificates.

   You can use the pre-defined **NGFW-Default-InternalCA** certificate, or click the menu and select Create or Choose to create a new certificate or select one you have already uploaded to the FDM-managed device.

   If you have not already installed the certificate in client browsers, click the download button to obtain a copy. See the documentation for each browser for information on how to install the certificate. Also see Downloading the CA Certificate for Decrypt Re-Sign Rules.

   Note You are prompted for SSL Decryption settings only if you have not already configured the SSL decryption policy. To change these settings after enabling the identity policy, edit the SSL decryption policy settings.

2. Click **Save**.

c) Click the **Server Certificate** menu to select (choose) the internal certificate to present to users during active authentication. If you have not already created the required certificate, click **Create**. Users will have to accept the certificate if you do not upload a certificate that their browsers already trust.

d) In the **Port** field, enter the port number for the captive portal. The default is 885 (TCP). If you configure a different port, it must be in the range 1025-65535.

Note For the HTTP Basic, HTTP Response Page, and NTLM authentication methods, the user is redirected to the captive portal using the IP address of the interface. However, for HTTP Negotiate, the user is redirected using the fully-qualified DNS name firewall-hostname.AD-domain-name . If you want to use HTTP Negotiate, you must also update your DNS server to map this name to the IP addresses of all inside interfaces where you are requiring active authentication. Otherwise, the redirection cannot complete, and users cannot authenticate.

e) Click **Save**.

Step 7 Continue with Configure the Identity Policy Default Action.

Configure the Identity Policy Default Action

The identity policy has a default action, which is implemented for any connections that do not match any individual identity rules.

In fact, having no rules is a valid configuration for your policy. If you intend to use passive authentication on all traffic sources, then simply configure Passive Authentication as your default action.

Procedure

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 Click **Identity** in the Policy bar.

Step 5 Configure Identity Policy Settings if you have not done so already.

Step 6 At the bottom of the screen, click the Default Action button and choose one of the following:

- **Passive Auth**—User identity will be determined using all configured passive identity sources for connections that do not match any identity rules. If you do not configure any passive identity sources, using Passive Auth as the default is the same as using No Auth.
- **No Auth**—User identity will not be determined for connections that do not match any identity rules.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Identity Rules

Identity rules determine whether user identity information should be collected for matching traffic. You can configure No Authentication if you do not want to collect user identity information for matching traffic.

Keep in mind that regardless of your rule configuration, active authentication is performed on HTTP traffic only. Thus, you do not need to create rules to exclude non-HTTP traffic from active authentication. You can simply apply an active authentication rule to all sources and destinations if you want to get user identity information for all HTTP traffic.

Note Also keep in mind that a failure to authentication has no impact on network access. Identity policies collect user identity information only. You must use access rules if you want to prevent users who failed to authenticate from accessing the network.

Procedure

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 Click **Identity** in the policy bar.

Step 5 Do any of the following:

- To create a new rule, click the plus button. To understand identity source objects and how they could affect your rules, see Configure Identity Sources for FDM-Managed Device for more information.
- To edit an existing rule, click the rule you want to edit and click **Edit** in the Actions pane at the right.
- To delete a rule you no longer need, click the rule you want to delete and click **Remove** in the Actions pane at the right.

Step 6 In **Order**, select where you want to insert the rule in the ordered list of rules.

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 7 In **Name**, enter a name for the rule.

Step 8 Select the **Action** that the FDM-managed device should apply on a match and if necessary, an Active Directory (AD) Identity Source.

You must select the AD identity realm that includes the user accounts for passive and active authentication rules. choose one of the following:

- **Passive Auth**—Use passive authentication to determine user identity. All configured identity sources are shown. The rule automatically uses all configured sources.
- **Active Auth**Use active authentication to determine user identity. Active authentication is applied to HTTP traffic only. If any other t—ype of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted.
- **No Auth**—Do not obtain user identity. Identity-based access rules will not be applied to this traffic. These users are marked as No Authentication Required.

Note For both **Passive Auth** and **Active Auth**, you can opt to select an AD Realm identity source. If you do not have any identity source objects readily prepared, click **Create new object** to launch the identity source object wizard. See Create or Edit an Active Directory Realm Object for more information.

Step 9 (Active Authentication only.) Click the **Active authentication** tab and select the authentication method (Type) supported by your directory server:

- **HTTP Basic**—Authenticate users using an unencrypted HTTP Basic Authentication connection. Users log in to the network using their browser's default authentication popup window. This is the default.
- **NTLM**—Authenticate users using an NT LAN Manager (NTLM) connection. This selection is only available when you select an AD realm. Users log in to the network using their browser's default authentication popup window, although you can configure Internet Explorer and Firefox browsers to transparently authenticate using their Windows domain login. That task is done in FDM, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Security Policies > Identity Policies > **Enabling Transparent User Authentication** for instructions.
- **HTTP Negotiate**—Allow the device to negotiate the method between the user agent (the application the user is using to initiate the traffic flow) and the Active Directory server. Negotiation results in the strongest commonly supported method being used, in order, NTLM, then basic. Users log in to the network using their browser's default authentication popup window.
- **HTTP Response Page**Prompt users to authenticate using a system-provided web page. This is a form of HTTP Basic authentication.

Note For the HTTP Basic, HTTP Response Page, and NTLM authentication methods, the user is redirected to the captive portal using the IP address of the interface. However, for HTTP Negotiate, the user is redirected using the fully-qualified DNS name *firewall-hostname.AD-domain-name* . If you want to use HTTP Negotiate, you must also update your DNS server to map this name to the IP addresses of all inside interfaces where you are requiring active authentication. Otherwise, the redirection cannot complete, and users cannot authenticate.

Step 10 (Active authentication only.) Select **Fall Back as Guest > On/Off** to determine whether users who fail active authentication are labeled as Guest users.

Users get 3 chances to successfully authenticate. If they fail, your selection for this option determines how the user is marked. You can deploy access rules based on these values.

- Fall Back as Guest > **On**—Users are marked as Guest.
- Fall Back as Guest > **Off**—Users are marked as Failed Authentication.

Step 11 Define the traffic matching criteria on the **Source** and **Destination** tabs for Passive authentication, Active authentication, or No Authentication rule actions.

Keep in mind that active authentication will be attempted with HTTP traffic only. Therefore, there is no need to configure No Auth rules for non-HTTP traffic, and there is no point in creating Active Authentication rules for any non-HTTP traffic. However, passive authentication is valid for any type of traffic.

The Source/Destination criteria of an identity rule define the security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the protocols and ports used in the traffic. The default is any zone, address, geographical location, protocol, and port.

To modify a condition, you click the  button within that condition, select the desired object or element, and click OK in the popup dialog box. If the criterion requires an object, you can click **Create New Object** if the object you require does not exist.

To remove an object from a condition, hover over the object and click the X.

You can configure the following traffic matching criteria.

Source Zones, Destination Zones

The security zone objects that define the interfaces through which the traffic passes. You can define one, both, or neither criteria: any criteria not specified applies to traffic on any interface.

- To match traffic leaving the device from an interface in the zone, add that zone to the Destination Zones.
- To match traffic entering the device from an interface in the zone, add that zone to the Source Zones.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones and egress through one of the destination zones.

Use this criteria when the rule should apply based on where the traffic enters or exits the device. For example, if you want to ensure that user identity is collected from all traffic originating from inside networks, select an inside zone as the Source Zones while leaving the destination zone empty.

Note You cannot mix passive and routed security zones in a single rule. In addition, you can specify passive security zones as source zones only, you cannot specify them as destination zones.

Source Networks, Destination Networks

The network objects or geographical locations that define the network addresses or locations of the traffic.

- To match traffic from an IP address or geographical location, configure the Source Networks.
- To match traffic to an IP address or geographical location, configure the Destination Networks.
- If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from the following tabs:

- **Network**â€”Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control.
- **Country/Continent**-Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent. Besides selecting geographical location directly in the rule, you can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.
- **Custom Geolocation**â€”Select (or create) a geolocation object that has exactly the countries and continents you specify.

Note To ensure you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB). See Create and Edit a Firepower Geolocation Filter Object for more information.

Source Ports, Destination Ports/Protocols

The port objects that define the protocols used in the traffic. For TCP/UDP, this can include ports.

- To match traffic from a protocol or port, configure the Source Ports. Source ports can be TCP/UDP only.
- To match traffic to a protocol or port, configure the Destination Ports/Protocols.
- To match traffic both originating from specific TCP/UDP ports and destined for specific TCP/UDP ports, configure both. If you add both source and destination ports to a condition, you can only add ports that

share a single transport protocol, TCP or UDP. For example, you could target traffic from port TCP/80 to port TCP/8080.

Step 12 Click **Save**.

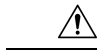
Step 13 Return to the **Inventory** page.

Step 14 Select the device to which you added these rules to the identity policy.

Step 15 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

SSL Decryption Policy

Some protocols, such as HTTPS, use Secure Sockets Layer (SSL) or its follow-on version, Transport Layer Security (TLS), to encrypt traffic for secure transmissions. Because the system cannot inspect encrypted connections, you must apply SSL decryption policy to decrypt them if you want to apply access rules that consider higher-layer traffic characteristics to make access decisions.



Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Continue with these topics:

- About SSL Decryption
- How to Implement and Maintain the SSL Decryption Policy
- Configure SSL Decryption Policies
- Configure Certificates for Known Key and Re-Sign Decryption
- Downloading the CA Certificate for Decrypt Re-Sign Rules
- Troubleshooting SSL Decryption Issues

How to Implement and Maintain the SSL Decryption Policy

You can use SSL decryption policies to turn encrypted traffic into plain text traffic, so that you can then apply URL filtering, intrusion and malware control, and other services that require deep packet inspection. If your policies allow the traffic, the traffic is re-encrypted before it leaves the device.

The SSL decryption policy applies to encrypted traffic only. No unencrypted connections are evaluated against SSL decryption rules.

Unlike some other security policies, you need to monitor and actively maintain the SSL decryption policy, because certificates can expire or even be changed on destination servers. Additionally, changes in client software might alter your ability to decrypt certain connections, because the decrypt re-sign action is indistinguishable from a man-in-the-middle attack.

The following procedure explains the end-to-end process of implementing and maintaining the SSL decryption policy.

Procedure

Procedure

Step 1 If you will implement Decrypt Re-sign rules, create the required internal CA certificate.

You must use an internal Certificate Authority (CA) certificate. You have the following options. Because users must trust the certificate, either upload a certificate client browsers are already configured to trust, or ensure that the certificate you upload is added to the browser trust stores.

- Create a self-signed internal CA certificate, which is signed by the device itself. See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Generating Self-Signed Internal and Internal CA Certificates.
- Upload an internal CA certificate and key signed by an external trusted CA or by a CA inside your organization. See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Uploading Internal and Internal CA Certificates.

Step 2 If you will implement Decrypt Known Key rules, collect the certificate and key from each of the internal servers.

You can use Decrypt Known Key only with servers that you control, because you must obtain the certificate and key from the server. Upload these certificates and keys as internal certificates (not internal CA certificates). See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Uploading Internal and Internal CA Certificates.

Step 3 Configure SSL Decryption Policies.

When you enable the policy, you also configure some basic settings.

Step 4 Configure the Default SSL Decryption Action

If in doubt, select Do Not Decrypt as the default action. Your access control policy can still drop traffic that matches the default SSL decryption rule if appropriate.

Step 5 Configure SSL Decryption Rules.

Identify traffic to decrypt and the type of decryption to apply.

Step 6 If you configure known key decryption, edit the SSL decryption policy settings to include those certificates. See Configure Certificates for Known Key and Re-Sign Decryption.

Step 7 If necessary, download the CA certificate used for Decrypt Re-sign rules and upload it to the browser on client workstations.

For information on downloading the certificate and distributing it to clients, see Downloading the CA Certificate for Decrypt Re-Sign Rules.

Step 8 Periodically, update re-sign known key certificates.

- Re-sign certificate—Update this certificate before it expires. If you generate the certificate through Firepower Device Manager, it is valid for 5 years. To determine when a certificate expires, click the view icon for the certificate from the Objects page.
- Known-key certificate—For any known-key decryption rules, you need to ensure that you have uploaded the destination server's current certificate and key. Whenever the certificate and key changes on supported

servers, you must also upload the new certificate and key (as an internal certificate) and update the SSL decryption settings to use the new certificate.

Step 9 Upload missing trusted CA certificates for external servers.

The system includes a wide range of trusted CA root and intermediate certificates issued by third parties. These are needed when negotiating the connection between FDM-managed devices and the destination servers for decrypt re-sign rules.

Upload all certificates within a root CA's chain of trust to the list of trusted CA certificates, including the root CA certificate and all intermediate CA certificates. Otherwise, it is more difficult to detect trusted certificates issued by intermediate CAs. Upload certificates on the Objects > Certificates page. See See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Uploading Trusted CA Certificates.

About SSL Decryption

Normally, the access control policy determines if network connections should be allowed or blocked. However, if you enable the SSL decryption policy, encrypted connections are first sent through the SSL decryption policy to determine if they should be decrypted or blocked. Any connections that were not blocked, whether or not decrypted, then go through the access control policy for a final allow/block decision.

Note You must enable the SSL decryption policy in order to implement active authentication rules in the identity policy. If you enable SSL decryption to enable identity policies, but do not otherwise want to implement SSL decryption, select Do Not Decrypt for the default action in the SSL Decryption page and do not create additional SSL decryption rules. The identity policy automatically generates whatever rules it needs.

The following topics explain encrypted traffic flow management and decryption in more detail.

- Why Implement SSL Decryption?
- Automatically Generated SSL Decryption Rules
- Handling Undecryptable Traffic

Why Implement SSL Decryption?

Encrypted traffic, such as HTTPS connections, cannot be inspected. Many connections are legitimately encrypted, such as connections to banks and other financial institutions. Many web sites use encryption to protect privacy or sensitive data. For example, your connection to Firepower Device Manager is encrypted. However, users can also hide undesirable traffic within encrypted connections.

By implementing SSL decryption, you can decrypt connections, inspect them to ensure they do not contain threats or other undesirable traffic, and then re-encrypt them before allowing the connection to proceed. (The decrypted traffic goes through your access control policy and matches rules based on inspected characteristics of the decrypted connection, not on the encrypted characteristics.) This balances your need to apply access control policies with the user's need to protect sensitive information.

You can also configure SSL decryption rules to block encrypted traffic of types you know you do not want on your network.

Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Actions You Can Apply to Encrypted Traffic

When configuring SSL decryption rules, you can apply the actions described in the following topics. These actions are also available for the default action, which applies to any traffic that does not match an explicit rule.

- Decrypt Re-Sign
- Decrypt Known Key
- Do Not Decrypt
- Block

Note Any traffic that passes through the SSL decryption policy must then pass through the access control policy. Except for traffic you drop in the SSL decryption policy, the ultimate allow or drop decision rests with the access control policy.

Decrypt Re-Sign

If you elect to decrypt and re-sign traffic, the system acts as a man-in-the-middle.

For example, the user types in https://www.cisco.com in a browser. The traffic reaches the FDM-managed device, the device then negotiates with the user using the CA certificate specified in the rule and builds an SSL tunnel between the user and the FDM-managed device. At the same time the device connects to https://www.cisco.com and creates an SSL tunnel between the server and the FDM-managed device.

Thus, the user sees the CA certificate configured for the SSL decryption rule instead of the certificate from www.cisco.com. The user must trust the certificate to complete the connection. The FDM-managed device then performs decryption/re-encryption in both directions for traffic between the user and destination server.

Note If the client does not trust the CA used to re-sign the server certificate, it warns the user that the certificate should not be trusted. To prevent this, import the CA certificate into the client trusted CA store. Alternatively, if your organization has a private PKI, you can issue an intermediate CA certificate signed by the root CA which is automatically trusted by all clients in the organization, then upload that CA certificate to the device.

If you configure a rule with the Decrypt Re-Sign action, the rule matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions. Because you can select a single re-sign certificate for the SSL decryption policy, this can limit traffic matching for resign rules.

For example, outgoing traffic encrypted with an elliptic curve (EC) algorithm matches a Decrypt Re-Sign rule only if the re-sign certificate is an EC-based CA certificate. Similarly, traffic encrypted with an RSA algorithm matches Decrypt Re-Sign rules only if the global re-sign certificate is RSA; outgoing traffic encrypted with an EC algorithm does not match the rule, even if all other configured rule conditions match.

Decrypt Known Key

If you own the destination server, you can implement decryption with a known key. In this case, when the user opens a connection to https://www.cisco.com, the user sees the actual certificate for www.cisco.com, even though it is the FDM-managed device that is presenting the certificate.

Your organization must be the owner of the domain and certificate. For the example of cisco.com the only possible way to have the end user see Cisco's certificate would be if you actually own the domain cisco.com (i.e. you are Cisco Systems) and have ownership of the cisco.com certificate signed by a public CA. You can only decrypt with known keys for sites that your organization owns.

The main purpose of decrypting with a known key is to decrypt traffic heading to your HTTPS server to protect your servers from external attacks. For inspecting client side traffic to external HTTPS sites, you must use decrypt re-sign as you do not own the servers.

Note To use known key decryption, you must upload the server's certificate and key as an internal identity certificate, and then add it to the list of known-key certificates in the SSL decryption policy settings. Then, you can deploy the rule for known-key decryption with the server's address as the destination address. For information on adding the certificate to the SSL decryption policy, see Configure SSL Decryption Policies.

Do Not Decrypt

If you elect to bypass decryption for certain types of traffic, no processing is done on the traffic. The encrypted traffic proceeds to the access control policy, where it is allowed or dropped based on the access control rule it matches.

Block

You can simply block encrypted traffic that matches an SSL decryption rule. Blocking in the SSL decryption policy prevents the connection from reaching the access control policy.

When you block an HTTPS connection, the user does not see the system default block response page. Instead, the user sees the browser's default page for a secure connection failure. The error message does not indicate the site was blocked due to policy. Instead, errors might indicate that there are no common encryption algorithms. It will not be obvious from this message that you blocked the connection on purpose.

Automatically Generated SSL Decryption Rules

Whether you enable the SSL decryption policy, FDM-managed device automatically generates Decrypt Re-sign rules for each identity policy rule that implements active authentication. This is required to enable active authentication for HTTPS connections.

When you enable the SSL decryption policy, you see these rules under the Identity Policy Active Authentication Rules heading. These rules are grouped at the top of the SSL decryption policy. The rules are read only. You can change them only by altering your identity policy

Handling Undecryptable Traffic

There are several characteristics that make a connection undecryptable. If a connection has any of the following characteristics, the default action is applied to the connection regardless of any rule the connection would otherwise match. If you select Block as your default action (rather than Do Not Decrypt), you might run into issues, including excessive drops of legitimate traffic.

- Compressed session—Data compression was applied to the connection.
- SSLv2 session—The minimum supported SSL version is SSLv3.
- Unknown cipher suite—The system does not recognize the cipher suite for the connection.
- Unsupported cipher suite—The system does not support decryption based on the detected cipher suite.
- Session not cached—The SSL session has session reuse enabled, the client and server reestablished the session with the session identifier, and the system did not cache that session identifier.
- Handshake errors—An error occurred during the SSL handshake negotiation.
- Decryption errors—An error occurred during the decryption operation.
- Passive interface traffic—All traffic on passive interfaces (passive security zones) is undecryptable.

License Requirements for SSL Decryption Policies

You do not need a special license to use the SSL decryption policy.

However, you do need the URL license to create rules that use URL categories and reputations as match criteria. For information on configuring licenses, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager> Licensing the System > Enabling or Disabling Optional Licenses.

Guidelines for SSL Decryption

Keep the following in mind when configuring and monitoring SSL decryption policies:

- The SSL Decryption policy is bypassed for any connections that match access control rules set to trust or block if those rules:
  - Use security zone, network, geolocation, and port only as the traffic matching criteria.
  - Come before any other rules that require inspection, such as rules that match connections based on application or URL, or allow rules that apply intrusion or file inspection.
- When using URL category matching, note that there are cases where the login page for a site is in a different category than the site itself. For example, Gmail is in the "Web based email" category, whereas the login page is in the "Internet Portals" category. To get connections to these sites decrypted, you must include both categories in the rule.

- You cannot disable the SSL decryption policy if you have any active authentication rules. To disable the SSL decryption policy, you must either disable the identity policy, or delete any identity rules that use active authentication.

Configure SSL Decryption Policies

You can use SSL decryption policies to turn encrypted traffic into plain text traffic, so that you can then apply URL filtering, intrusion and malware control, and other services that require deep packet inspection. If your policies allow the traffic, the traffic is re-encrypted before it leaves the device.

The SSL decryption policy applies to encrypted traffic only. No unencrypted connections are evaluated against SSL decryption rules.

Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Note VPN tunnels are decrypted before the SSL decryption policy is evaluated, so the policy never applies to the tunnel itself. However, any encrypted connections within the tunnel are subject to evaluation by the SSL decryption policy.

The following procedure explains how to configure the SSL decryption policy. For an explanation of the end-to-end process of creating and managing SSL decryption, see How to Implement and Maintain the SSL Decryption Policy.

Procedure

Before you begin

The SSL decryption rules table contains two sections:

- **Identity Policy Active Authentication Rules**—If you enable the identity policy and create rules that use active authentication, the system automatically creates the SSL decryption rules needed to make those policies work. These rules are always evaluated before the SSL decryption rules you create yourself. You can alter these rules only indirectly, by making changes to the identity policy.
- **SSL Native Rules**—These are rules that you have configured. You can add rules to this section only.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to create the SSL policy.

Step 4 Click **Policy** in the **Management** pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 If you have not yet enabled the policy, click **Enable SSL Decryption** and configure policy settings, as described in Enable the SSL Decryption Policy.

Step 7 Configure the default action for the policy. The safest choice is Do Not Decrypt. For more information, see **Configure the Default SSL Decryption Action** section of the Security Policies chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Step 8 Manage the SSL decryption policy.

After you configure SSL decryption settings, this page lists all rules in order. Rules are matched against traffic from top to bottom with the first match determining the action to apply. You can do the following from this page:

- To disable the policy, click the SSL Decryption Policy toggle. You can re-enable it by clicking Enable SSL Decryption.
- To edit policy settings, including the list of certificates used in the policy, click the configuration button on the SSL toolbar: 

. You can also download the certificate used with decrypt re-sign rules so that you can distribute it to clients. See the following sections of the Security Policies chapter in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager of the version your device is running:
  - Configure Certificates for Known Key and Re-Sign Decryption
  - Downloading the CA Certificate for Decrypt Re-Sign Rules
- To configure rules:
  - To create a new rule and log events it generates, click the blue plus button  . See Configure SSL Decryption Rules.
  - To edit an existing rule, click the rule in the rule table and click **Edit** in the Actions pane. You can also selectively edit a rule property by clicking on the property in the table.
  - To delete a rule you no longer need, click the rule in the rule table and click **Remove** in the Actions pane.
  - To move a rule, hover over it in the rule table. At the end of the row use the up and down arrows to move its position with the rule table.
  - (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 9 Continue to Enable the SSL Decryption Policy.

Enable the SSL Decryption Policy

Before you can configure SSL decryption rules, you must enable the policy and configure some basic settings. The following procedure explains how to enable the policy directly. You can also enable it when you enable identity policies. Identity policies require that you enable the SSL decryption policy.

Procedure

Before you begin

If you upgraded from a release that did not have SSL decryption policies, but you had configured the identity policy with active authentication rules, the SSL decryption policy is already enabled. Ensure that you select the Decrypt Re-Sign certificate you want to use, and optionally enable pre-defined rules.

Review Configure SSL Decryption Policies if you have not already.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and the device for which you want to enable the SSL Decryption policy.

Step 4 Click **Policy** in the **Management** pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 Click the **SSL Decryption** toggle in the SSL bar to enable the SSL Decryption policy.

- If this is the first time you enabled the policy, read the description of Decrypt Known-Key and Decrypt Re-Sign SSL decryption and click enable.
- If you have already configured the policy once and then disabled it, the policy is simply enabled again with your previous settings and rules. You can click the SSL decryption configuration button 

Configure Certificates for Known Key and Re-Sign Decryption and configure settings as described in .

Step 7 For **Select Decrypt Re-Sign Certificate**, select the internal CA certificate to use for rules that implement decryption with re-signed certificates.

You can use the pre-defined NGFW-Default-InternalCA certificate, or one that you created or uploaded. If the certificate does not yet exist, click **Create** to add an FDM-managed device internal CA certificate.

If you have not already installed the certificate in client browsers, click the download button  to obtain a copy. See the documentation for each browser for information on how to install the certificate. Also see Downloading the CA Certificate for Decrypt Re-Sign Rules

Step 8 Click **Save.**

Step 9 Continue with Configure the Default SSL Decryption Action to set the default action for the policy.

Configure the Default SSL Decryption Action

If an encrypted connection does not match a specific SSL decryption rule, it is handled by the default action for the SSL decryption policy.

Procedure

Before you begin

If you have not already, review these procedures and follow the procedures in them:

1. Configure SSL Decryption Policies
2. Enable the SSL Decryption Policy

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to configure the default SSL decryption action.

Step 4 Click **Policy** in the **Management** pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 Click the **Default Action** button.

Step 7 Select the action to apply to matching traffic:

- **Do Not Decrypt**—Allow the encrypted connection. The access control policy then evaluates the encrypted connection and drops or allows it based on access control rules.
- **Block**—Drop the connection immediately. The connection is not passed on to the access control policy.

Step 8 (Optional.) Configure logging for the default action. You must enable logging to capture events from SSL Decryption policies. Select from these options:

- **At End of Connection**—Generate an event at the conclusion of the connection.
  - Send Connection Events Toâ€"If you want to send a copy of the events to an external syslog server, select the server object that defines the syslog server. If the required object does not already exist, click Create New Syslog Server and create it. (To disable logging to a syslog server, select Any from the server list.)

    Because event storage on the device is limited, sending events to an external syslog server can provide more long term storage and enhance your event analysis.

    If you have a subscription to Cisco Security Analytics and Logging, Send FDM Events to Security Cloud Control Events Logging. See Secure Logging Analytics for FDM-Managed Devices for more information about this feature.
- **No Logging**—Do not generate any events.

Step 9 Click **Save.**

Step 10 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure SSL Decryption Rules

Use SSL decryption rules to determine how to handle encrypted connections. Rules in the SSL decryption policy are evaluated from top to bottom. The rule applied to traffic is the first one where all the traffic criteria are matched.

You can create and edit rules in the SSL Native Rules section only.

Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Note Traffic for your VPN connections (both site-to-site and remote access) is decrypted before the SSL decryption policy evaluates connections. Thus, SSL decryption rules are never applied to VPN connections, and you do not need to consider VPN connections when creating these rules. However, any use of encrypted connections within a VPN tunnel are evaluated. For example, an HTTPS connection to an internal server through an RA VPN connection is evaluated by SSL decryption rules, even though the RA VPN tunnel itself is not (because it is decrypted already)

Procedure

Before you begin

If you have not already, review Configure SSL Decryption Policies, Enable the SSL Decryption Policy, and Configure the Default SSL Decryption Action to configure the SSL decryption policy your rules will be added to.

If you are creating a decrypt known-key rule, ensure that you upload the certificate and key for the destination server (as an internal certificate) and also edit the SSL decryption policy settings to use the certificate. Known-key rules typically specify the destination server in the destination network criteria of the rule. For more information, see Configure Certificates for Known Key and Re-Sign Decryption.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to enable the SSL Decryption policy.

Step 4 Click **Policy** in the Management pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 Do any of the following:

- To create a new rule, click the blue plus button.
- To edit an existing rule, click the edit icon for the rule.
- To delete a rule you no longer need, click the remove icon for the rule.

Step 7 In **Order**, select where you want to insert the rule in the numbered list of rules.

You can insert rules into the SSL Native Rules section only. The Identity Policy Active Authentication Rules are automatically generated from your identity policy and are read-only.

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 8 In **Name**, enter a name for the rule.

The name cannot contain spaces. You can use alphanumeric characters and these special characters: + . _ -

Step 9 Select the action to apply to matching traffic. For a detailed discussion of each option, see the following:

- Decrypt Re-Sign
- Decrypt Known Key
- Do Not Decrypt
- Block

Step 10 Define the traffic matching criteria using any combination of the following tabs:

- **Source/Destination**—The security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the TCP ports used in the traffic. The default is any zone, address, geographical location, and TCP port. See Source/Destination Criteria for SSL Decryption Rules.
- **URL**—The URL category of a web request. The default is that the URL category and reputation are not considered for matching purposes. See URL Criteria for SSL Decryption Rules
- **Application**—The application, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any encrypted application. See Application Criteria for SSL Decryption Rules .
- **Users**—The user or user group. Your identity policies determine whether user and group information is available for traffic matching. You must configure identity policies to use this criteria. See User Criteria for SSL Decryption Rules.
- **Advanced**—The characteristics derived from the certificates used in the connection, such as SSL/TLS version and certificate status. See Advanced Criteria for SSL Decryption Rules.

To modify a condition, you click the blue plus button  within that condition, select the desired object or element, and click **Select** in the popup dialog box. If the criterion requires an object, you can click **Create New Object** if the object you require does not exist. Click the x for an object or element to remove it from the policy.

When adding conditions to SSL decryption rules, consider the following tips:

- You can configure multiple conditions per rule. Traffic must match all the conditions in the rule for the rule to apply to traffic. For example, you can use a single rule to decrypt traffic based on URL category.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches any of a condition's criteria satisfies the condition. For example, you can use a single rule to apply application control for up to 50

applications or application filters. Thus, there is an OR relationship among the items in a single condition, but an AND relationship between condition types (for example, between source/destination and application).

- Matching URL category requires the URL license.

Step 11 (Optional.) Configure logging for the rule.

You must enable logging for traffic that matches the rule to be included in dashboard data or Event Viewer. Select from these options:

- **No logging**—Do not generate any events.
- **Send Connection Events To**—If you want to send a copy of the events to an external syslog server, select the server object that defines the syslog server. If the required object does not already exist, click **Create** and create it. (To disable logging to a syslog server, select Any from the server list.)
- **At End of Connection**—Generate an event at the conclusion of the connection. Because event storage on the device is limited, sending events to an external syslog server can provide more long term storage and enhance your event analysis.

If you have a subscription to Cisco Security Analytics and Logging, specify or Create a Syslog Server Object for Secure Logging Analytics (SaaS) using a Secure Event Connector's IP address and port. See Cisco Security Analytics and Logging for more information.

Step 12 Click **Save**.

Step 13 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Source/Destination Criteria for SSL Decryption Rules

The Source/Destination criteria of an SSL decryption rule define the security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the TCP ports used in the traffic. The default is any zone, address, geographical location, and any TCP port. TCP is the only protocol matched to SSL decryption rules.

To modify a condition, you click the blue button  within that condition, select the desired object or element, and click **Select**. If the criterion requires an object, you can click **Create New Object** if the object you require does not exist. Click the **x** for an object or element to remove it from the policy.

Source Zones, Destination Zones

The security zone objects that define the interfaces through which the traffic passes. You can define one, both, or neither criteria: any criteria not specified applies to traffic on any interface.

- To match traffic leaving the device from an interface in the zone, add that zone to the Destination Zones.
- To match traffic entering the device from an interface in the zone, add that zone to the Source Zones.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones and egress through one of the destination zones.

Use this criteria when the rule should apply based on where the traffic enters or exits the device. For example, if you want to ensure that all traffic going from outside hosts to inside hosts gets decrypted, you would select your outside zone as the Source Zones and your inside zone as the Destination Zones.

Source Networks, Destination Networks

The network objects or geographical locations that define the network addresses or locations of the traffic.

- To match traffic from an IP address or geographical location, configure the Source Networks.
- To match traffic to an IP address or geographical location, configure the Destination Networks.

If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from the following menu options:

- **Network**—Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control.

Note For Decrypt Known-Key rules, select an object with the IP address of the destination server that uses the certificate and key you uploaded.

- **Country/Continent**—Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent.
- **Custom Geolocation**-You can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

Source Ports, Destination Ports/Protocols

The port objects that define the protocols used in the traffic. You can specify TCP protocol and ports only for SSL decryption rules.

- To match traffic from a TCP port, configure the Source Ports.
- To match traffic to a TCP port, configure the Destination Ports/Protocols.

To match traffic both originating from specific TCP ports and destined for specific TCP ports, configure both. For example, you could target traffic from port TCP/80 to port TCP/8080.

Step 10

Application Criteria for SSL Decryption Rules

The Application criteria of an SSL decryption rule defines the application used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application that has the SSL Protocol tag. You cannot match SSL decryption rules to any non-encrypted application.

Although you can specify individual applications in the rule, application filters simplify policy creation and administration. For example, you could create an SSL decryption rule that decrypts or blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is decrypted or blocked.

In addition, Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule for high risk applications can automatically apply to new applications without you having to update the rule manually.

You can specify applications and filters directly in the rule, or create application filter objects that define those characteristics. The specifications are equivalent, although using objects can make it easier to stay within the 50-items-per-criteria system limit if you are creating a complex rule.

To modify the application and filters list, you click the  button within the condition, select the desired applications or application filter objects, and click Select in the popup dialog box and then click Save. Click the x for an application, filter, or object to remove it from the policy. Click the Save As Filter link to save the combined criteria that is not already an object as a new application filter object.

For more information about the application criteria and how to configure advanced filters and select applications, see Create and Edit a Firepower Application Filter Object.

Consider the following tips when using application criteria in SSL decryption rules:

- The system can identify unencrypted applications that become encrypted using StartTLS. This includes such applications as SMTPS, POPS, FTPS, TelnetS, and IMAPS. In addition, it can identify certain encrypted applications based on the Server Name Indication in the TLS ClientHello message, or the server certificate subject distinguished name value.
- The system can identify the application only after the server certificate exchange. If traffic exchanged during the SSL handshake matches all other conditions in an SSL rule containing an application condition but the identification is not complete, the SSL policy allows the packet to pass. This behavior allows the handshake to complete so that applications can be identified. After the system completes its identification, the system applies the SSL rule action to the remaining session traffic that matches its application condition.

Step 10

URL Criteria for SSL Decryption Rules

The URL criteria of an SSL decryption rule defines the category to which the URL in a web request belongs. You can also specify the relative reputation of sites to decrypt, block, or allow without decryption. The default is to not match connections based on URL categories.

For example, you could block all encrypted Gaming sites, or decrypt all high risk Social Networking sites. If a user attempts to browse to any URL with that category and reputation combination, the session is blocked or decrypted.

To add URL criteria to an SSL decryption rule:

Procedure

Step 1 Click the URL tab to add a URL category to an SSL Decryption rule.

Step 2 Search for and select the URL categories you want to block.

Step 3 By default, the traffic from URLs in the categories you pick will be decrypted by the SSL decryption rule no matter their security reputation. However, you can fine-tune the URL category or all the URL categories in your rule to exclude some sites from decryption based on reputation.

- To fine-tune the reputation of a single category in the URL:

a. Click the URL category after you selected it.

b. Uncheck **Any Reputation**.

c. Slide the green slider to the right to choose the URL reputation settings you want to exclude from the rule and click **Save**.

   The reputations that the slider covers are excluded from the effect of the rule. For example, if you slide the green slider to Benign Sites, Well Known Sites and Benign Sites are excluded from the effects of the SSL Decryption rule for the category you chose. URLs deemed to be Sights with Security Risks, Suspicious Sites, and High Risk Sites will still be affected by the rule for that URL category.

- To fine-tune the reputation of all the URL categories you added to the rule:

  a. After you have selected all the categories you want to include in the SSL Decryption rule, click **Apply Reputation to Selected Categories**.

  b. Uncheck **Any Reputation**.

  c. Slide the green slider to the right to choose the URL reputation settings you want to exclude from the rule and click **Save**.

     The reputations that the slider covers are excluded from the effect of the rule. For example, if you slide the green slider to Benign Sites, Well Known Sites and Benign Sites are excluded from the effects of the SSL Decryption rule for all the categories you chose. URLs deemed to be Sights with Security Risks, Suspicious Sites, and High Risk Sites will still be affected by the rule for all the URL categories.

Step 4 Click **Select**.

Step 5 Click **Save**.

Step 10

User Criteria for SSL Decryption Rules

The User criteria of an SSL decryption rule defines the user or user group for an IP connection. You must configure identity policies and the associated directory server to include user or user group criteria in a rule.

Your identity policies determine whether user identity is collected for a particular connection. If identity is established, the IP address of the host is associated with the identified user. Thus, traffic whose source IP address is mapped to a user is considered to be from that user. IP packets themselves do not include user identity information, so this IP-address-to-user mapping is the best approximation available.

Because you can add a maximum of 50 users or groups to a rule, selecting groups usually makes more sense than selecting individual users. For example, you could create a rule that decrypts traffic to the Engineering group that comes from the outside network, and create a separate rule that does not decrypt outgoing traffic from that group. Then, to make the rule apply to new engineers, you only need to add the engineer to the Engineering group in the directory server.

To modify the users list, you click the + button within the condition and select the desired user groups and click Select.

Step 10

Advanced Criteria for SSL Decryption Rules

The Advanced traffic matching criteria relate to characteristics derived from the certificates used in the connection. You can configure any or all of the following options.

Certificate Properties

Traffic matches the certificate properties option of the rule if it matches any of the selected properties. You can configure the following:

- **Certificate Status**: Whether the certificate is Valid or Invalid. Select Any (the default) if you do not care about certificate status. A certificate is considered valid if all of the following conditions are met, otherwise it is invalid:
  - The policy trusts the CA that issued the certificate.
  - The certificate's signature can be properly validated against the certificate's content.
  - The issuer CA certificate is stored in the policy's list of trusted CA certificates.
  - None of the policy's trusted CAs revoked the certificate.
  - The current date is between the certificate Valid From and Valid To dates.
- **Self-Signed**: Whether the server certificate contains the same subject and issuer distinguished name. Select one of the following:
- Self-Signing—The server certificate is self-signed.
  - CA-Signing—The server certificate is signed by a Certificate Authority. That is, the issuer and subject are not the same.
  - Any—Do not consider whether the certificate is self-signed as a match criteria.

Supported Version

The SSL/TLS version to match. The rule applies to traffic that uses the any of the selected versions only. The default is all versions. Select from: SSLv3.0, TLSv1.0, TLSv1.1, TLSv1.2.

For example, if you wanted to permit TLSv1.2 connections only, you could create a block rule for the non-TLSv1.2 versions. Traffic that uses any version not listed, such as SSL v2.0, is handled by the default action for the SSL decryption policy.

Step 10

Configure Certificates for Known Key and Re-Sign Decryption

If you implement decryption, either by re-signing or using known keys, you need to identify the certificates that the SSL decryption rules can use. Ensure that all certificates are valid and unexpired.

Especially for known-key decryption, you need to ensure that the system has the current certificate and key for each destination server whose connections you are decrypting. With a decrypt known key rule, you use the actual certificate and key from the destination server for decryption. Thus, you must ensure that the FDM-managed device has the current certificate and key at all times, or decryption will be unsuccessful.

Upload a new internal certificate and key whenever you change the certificate or key on the destination server in a known key rule. Upload them as an internal certificate (not an internal CA certificate). You can upload

the certificate during the following procedure, or upload the certificate to the **Objects** page by clicking the  button and selecting **FTD > Certificate**.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to create the SSL policy and click **Policy** in the Management pane at the right.

Step 4 Click **SSL Decryption** in the policy bar.

Step 5 Click the certificate button 

in the SSL decryption policy policy bar.

Step 6 In the SSL Decryption Configuration dialog, click the **Select Decrypt Re-Sign Certificate** menu and select or create the internal CA certificate to use for rules that implement decryption with re-signed certificates. You can use the pre-defined **NGFW-Default-InternalCA** certificate, or one that you created or uploaded.

If you have not already installed the certificate in client browsers, click the download button  to obtain a copy. See the documentation for each browser for information on how to install the certificate. Also see the **Downloading the CA Certificate for Decrypt Re-Sign Rules** section of the Security Policies chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running

Step 7 For each rule that decrypts using a known key, upload the internal certificate and key for the destination server.

Step 8 Click  under **Decrypt Known-Key Certificates**.

Step 9 Select the internal identity certificate, or click **Create New Internal Certificate** to upload it now.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Downloading the CA Certificate for Decrypt Re-Sign Rules

If you decide to decrypt traffic, users must have the internal CA certificate that is used in the encryption process defined as a Trusted Root Certificate Authority in their applications that use TLS/SSL. Typically if you generate a certificate, or sometimes even if you import one, the certificate is not already defined as trusted in these applications. By default in most web browsers, when users send HTTPS requests, they will see a warning message from the client application informing them that there is a problem with the web site's security certificate. Usually, the error message says that the web site's security certificate was not issued by a trusted certificate authority or the web site was certified by an unknown authority, but the warning might also suggest there is a possible man-in-the-middle attack in progress. Some other client applications do not show this warning message to users nor allow users to accept the unrecognized certificate.

You have the following options for providing users with the required certificate:

Inform users to accept the root certificate

You can inform the users in your organization what the new policies are at the company and tell them to accept the root certificate supplied by the organization as a trusted source. Users should accept the certificate and save it in the Trusted Root Certificate Authority storage area so that they are not prompted again the next time they access the site.

Note The user needs to accept and trust the CA certificate that created the replacement certificate. If they instead simply trust the replacement server certificate, they will continue to see warnings for each different HTTPS site that they visit.

Add the root certificate to client devices

You can add the root certificate to all client devices on the network as a trusted root certificate authority. This way, the client applications automatically accept transactions with the root certificate.

You can either make the certificate available to users by E-mailing it or placing it on a shared site, or you could incorporate the certificate into your corporate workstation image and use your application update facilities to distribute it automatically to users.

The following procedure explains how to download the internal CA certificate and install it on Windows clients.

Procedure

The process differs depending on the operating system and type of browser. For example, you can use the following process for Internet Explorer and Chrome running on Windows. (For Firefox, install through the **Tools** > **Options** > **Advanced** page.)

Messages should indicate that the import was successful. You might see an intermediate dialog box warning you that Windows could not validate the certificate if you generated a self-signed certificate rather than obtaining one from a well-known third-party Certificate Authority.

You can now close out the Certificate and Internet Options dialog boxes.

Procedure

Step 1 Download the certificate from Firepower Device Manager.

a) In the left pane, click **Security Devices**.
b) Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
c) Click the **FTD** tab and select the device on which the certificate is stored.
d) Click **Policy** in the Management pane at the right.
e) Click **SSL Decryption** in the policy bar.
f) Click the SSL decryption configuration button 

in the SSL decryption policy policy bar.
g) Click the Download button 
h) Select a download location, optionally change the file name (but not the extension), and click Save.
i) You can now cancel out of the SSL Decryption Settings dialog box.

Step 2 Install the certificate in the Trusted Root Certificate Authority storage area in web browsers on client systems, or make it available for clients to install themselves. This procedure will be different for different browsers and operating systems.

Warning

CA Certificates Configured Through FDM-Managed Devices

Security Cloud Control can manage multiple devices but is limited the in additional information that is saved when the device configuration is saved, which may incur some issues when handling internal CA certificates. Security Cloud Control **does not** save the cert or key information of CA certificates that are configured through the FDM-managed console; if you attempt to use a CA certificate that was configured in an FDM-managed device and apply it to an SSL policy that is deployed to a secondary device, Security Cloud Control creates a local copy of the CA certificate but does not and cannot copy the key information. As a result, neither Security Cloud Control or the secondary device have the key information and the CA certificate cannot be successfully deployed. This also means that the download link for the local copy of the CA certificate is unavailable.

We strongly recommend configuring a separate CA certificate for any additional devices through an FDM-managed device, or creating CA certificates through the Security Cloud Control UI.

Rulesets

About Rulesets

A ruleset is a collection of access control rules that can be shared with multiple FDM-managed devices. Any changes made to the rules of a ruleset affect the other managed devices that use this ruleset. An FDM-managed device can have device-specific (local) and shared (rulesets) rules. You can also create rulesets from existing rules in an FDM-managed device.

Important The "Rulesets" feature is currently available FDM-managed devices Upgrade a Single FDM-Managed Device and later. Also note that rulesets do not support devices enabled for Snort 3.

The following limitations apply:

- You cannot attach rulesets to Snort 3-enabled devices.
- You cannot create a ruleset from an existing device that has Snort 3 installed.
- You cannot associate a custom IPS policy with a ruleset.

Copy or Move Rules associated with Rulesets

It's possible to copy or move access control rules within a ruleset or across different rulesets. Also, you're allowed to copy or move rules between local and rulesets. See Copy FDM-Managed Access Control Rules and Move FDM-Managed Access Control Rules for more information.

Auto-Detect Existing Rulesets

When you onboard a device, Security Cloud Control auto-detects existing rulesets on them and tries to match them with the rules on the device. On a successful match, Security Cloud Control automatically attaches the rulesets to the newly onboarded device. However, if there are multiple ruleset matches for the same set of rules on the device, none of them are attached, and you have to assign them manually.

Configure Rulesets for a Device

Use the sections below to create and deploy a ruleset:

Procedure

Step 1 Configure Rulesets for a Device.

a) Create a new ruleset and assign rules to it.
b) Assign objects to the rules.
c) Set the priority of the ruleset.
d) Change the order of the rules if required.

Step 2 Configure Rulesets for a Device.

a) Attach multiple devices to a ruleset.
b) Review and deploy the ruleset to the devices.

Create or Edit a Ruleset

You can create a ruleset and add new access control rules to it.

Use the following procedure to create a ruleset for multiple FDM-managed devices:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**.

Step 2 Click the plus  button to create a new ruleset.

Note To edit an existing ruleset, select the ruleset and click the edit icon .

Step 3 Enter a name for the ruleset and then click **Create**.

Step 4 Create access control rules to add them to the ruleset. See Configure the FDM Access Control Policy for instructions.

Note Access Control rules in the rulesets don't support criteria for Users criteria.

Step 5 In the upper right corner of the window, select the ruleset's priority 

. The priority can be set when the device is not attached to the ruleset. This selection affects all of the rules included in this ruleset and how it is handled on the devices:

- **Top**- The ruleset is processed before all other rules on the device. Rules are ordered at the top of the rule list and are processed first. No other ruleset can precede the rules in this policy. You can only have one top ruleset per device.
- **Bottom**- The ruleset is processed after all other rules on the device. Other than the policy's default action, no other ruleset can succeed rules in this policy. You can only have one bottom ruleset per device. By default, the priority is set to **Bottom**.

The **Local Rules** displays all the device-specific rules of the device.

Note The priority cannot be changed when a ruleset is attached to a device. You have to detach the device and change the priority.

Step 6 Click **Save**. You can create as many rules as you want.

Step 7 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Note
- You can change the order of rules in a ruleset even if you have devices attached to the ruleset. Use the following procedure to change the priority of the ruleset:
  a. In the navigation pane, click **Policies** > **Rulesets** and select the ruleset you want to modify.
  b. Select a rule that you want to move.
  c. Hover the cursor inside the rule row and use the **Move Up** or **Move Down** arrow to move the rule to the desired order.
- Security Cloud Control allows you to Object Overrides associated with the rules of a ruleset. When you add a new object to a rule, you can override it only after you attach a device to the ruleset and save the changes.

Deploy a Ruleset to Multiple FDM-Managed Devices or Templates

You must attach a ruleset to a device or template for the rules to be enforced. After reviewing the changes, you can deploy the configuration on the device. When you apply a template to a new FDM-managed device, the ruleset included in the template is pushed to the device.

For more information, see Rulesets with FDM-Managed Templates.

Before you begin, consider the following information:

- You can only attach a ruleset to FDM-managed devices that are already onboarded to Security Cloud Control.
- A device can have only **one** bottom or top ruleset.
- After you attach or remove a device from a ruleset, the changes are staged in Security Cloud Control but not deployed, and the device becomes **Not Synced** with Security Cloud Control. Deploy the changes to the device by clicking the icon from the top right corner of the screen.
- After you attach a device, the new rules associated with rulesets don't overwrite existing rules associated with the device.

You can associate rulesets with devices in two ways:

- Add devices to a Ruleset from the Ruleset page.
- Add Rulesets to a device from the Device Policy page.

Add Devices to a Ruleset from the Ruleset page

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**.

Step 2 Select the ruleset you want to assign to FDM-managed devices and in the **Actions** pane, click **Edit**.

Step 3 On the top right corner, click the **Device** button 

appearing beside **Ruleset for**.

Step 4 Select from the list of eligible FDM-managed devices.

Step 5 In the gear icon, select one of the following actions for the system to perform when it determines duplicate names between the rules in the ruleset and the device-specific rules:

- **Fail on conflicting rules** (default option): Security Cloud Control doesn't add the ruleset to the device. You need to manually rename the duplicate rules and then add the ruleset.
- **Rename conflicting rules**: Security Cloud Control renames the conflicting rules present on the device (Local Rules).

Step 6 Click **Save**. The **Attached Ruleset to Devices** wizard is closed.

Step 7 Click **Save** in the upper right corner to save the changes made to the ruleset. Saving the ruleset stages the changes to Security Cloud Control.

Note Each time you modify a ruleset, you must click **Save**. By doing this operation, all changes are staged to Security Cloud Control. You have to deploy the changes manually.

Step 8 Click **Confirm**. Saving the ruleset stages the changes to Security Cloud Control.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once. If you Discard Configuration Changes the staged ruleset changes on a device, see Impact of Discarding Staged Ruleset Changes for information.

Add Rulesets to a Device from the Device Policy page

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want from the list.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Click the  button appearing in the upper right corner of the window.

Step 6 Select the rulesets that you want.

Step 7 In the gear icon, select one of the following actions for the system to perform when it determines duplicate names between the rules in the ruleset and the device-specific rules:

- **Fail on conflicting rules** (default option): Security Cloud Control doesn't add the ruleset to the device. You need to manually rename the duplicate rules and then add the ruleset.
- **Rename conflicting rules**: Security Cloud Control renames the conflicting rules present on the device (Local Rules).

Note If there are no conflicting rules on the selected device, Security Cloud Control attaches the ruleset to the device without any changes.

Step 8 Click **Attach Ruleset**. The ruleset gets added to the device based on the priority of the ruleset.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once. If you Discard Configuration Changes the staged ruleset changes on a device, see Impact of Discarding Staged Ruleset Changes for information.

Related Information:

- Rulesets
- Rulesets with FDM-Managed Templates
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Create Rulesets from Existing Device Rules

Rulesets with FDM-Managed Templates

Security Cloud Control allows you to assign the rulesets to FDM-managed templates.

- When you create a template from an FDM-managed device with rulesets, Security Cloud Control adds the template automatically to the rulesets that were present on the source device. You can manage the template from rulesets.
- When you apply a template with rulesets to a target FDM-managed device, Security Cloud Control adds the target device automatically to the rulesets, thereby manage the target device from rulesets.
- When a template with rulesets is applied to a target FDM-managed device which already has different rulesets, Security Cloud Control removes the existing rulesets from the target device and adds new rulesets associated with the template.

See Deploy a Ruleset to Multiple FDM-Managed Devices or Templates for more information.

Related Information:

- Rulesets

Create Rulesets from Existing Device Rules

You're allowed to create rulesets by selecting existing rules in the FDM-managed device.

Use the following procedure to create a ruleset from existing device rules:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 In the **Management** pane on the right, click **Policy**. The existing rules of the device appear.

Step 5 Perform the following based on your requirement:

a) To create **Top** rules, select consecutive rules starting from the first rule at the top.

b) To create **Bottom** rules, select consecutive rules that include the last rule at the bottom.

Step 6 In the **Actions** pane on the right, click **Create Ruleset**.

Note Your selection must include the first or last rule for the **Create Ruleset** link to be clickable.

Step 7 Specify a name in the **Ruleset Name** field and click **Create**. The corresponding ruleset is created in the device.

You can continue creating ruleset using the remaining rules in the device.

Impact of Out-of-Band Changes on Rulesets

When you add new rules or make changes to the existing rules using the FDM-managed device, and you have enabled conflict detection in Security Cloud Control for your FDM-managed device, Security Cloud Control detects the out-of-band change and the device's configuration status shows **Conflict Detected**. Resolve Configuration Conflicts.

If you accept the device changes, Security Cloud Control overwrites the last know configuration with the new changes made on the device. The following changes take place:

- Rulesets that are impacted by the changes lose their relationship with devices.
- Rules associated with these rulesets are converted to local rules.

If you reject the device changes, Security Cloud Control rejects the new changes and replaces configuration on the device with the last synced configuration in Security Cloud Control.

Related Information:

- Rulesets
- Configure Rulesets for a Device
- Create Rulesets from Existing Device Rules
- Impact of Discarding Staged Ruleset Changes
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets

Impact of Discarding Staged Ruleset Changes

When you add new rules to a ruleset or make changes to the existing rules associated with the ruleset using Security Cloud Control, it saves the changes you make to its own copy of the configuration file. Those changes are considered "pending" on Security Cloud Control until they are "deployed" to the device.

If you Discard Configuration Changes the pending ruleset changes on the device, Security Cloud Control **completely overwrites** its local copy of a device's configuration with the configuration stored on the device.

The following changes occur on the rulesets and the associated devices:

- Rulesets that are impacted by the changes lose their relationship with devices.
- Rules associated with these rulesets are converted to local rules.
- Security Cloud Control discards the new staged changes and retains the configuration present on the device.

Related Information:

- Rulesets
- Configure Rulesets for a Device
- Create Rulesets from Existing Device Rules
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets

View Rules and Rulesets

View Rules from Device Policy Page

The FDM-managed device policy page shows individual (local) and shared rules (associated with rulesets).

Use the following procedure to view the FDM-managed device ruleset from the policy page:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want.

Step 4 In the **Management** pane on the right, click **Policy**. You see the following rules based on the configuration you have made:

- **Top Rules**: Shows the mandatory shared rules which will be processed before all other rules on the device.
- **Local Rules**: Shows device-specific rules which will be processed after mandatory rules on the device.
- **Bottom**: Shows the default shared rules which will be processed after all other rules on the device.

Note You can edit the ruleset by going to the corresponding ruleset page.

a) On the top right corner of the ruleset header, click **Go to ruleset**  .

b) Make the required changes to the rules and click **Save**. The new changes are updated on all devices associated with the ruleset.

View Rulesets

The **Rulesets** page shows all rulesets available in your tenant. It also provides information about devices associated with the rulesets.

Use the following procedure to view all rulesets from the Rulesets page:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click a ruleset to view its details. The **Devices** column shows the number of FDM-managed devices attached to each ruleset.

Step 3 In the **Management** pane, click **Workflows**. This page shows all the actions that you performed on the device. You can click **Diagram** to view a pictorial representation of the workflow.

Search Rulesets

You can use the **Filter by Device** filter to select the devices for viewing the rulesets assigned to them.

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click the filter icon and click **Filter by Device**.

Step 3 Select one or more devices from the list and click **OK**.

You can see the rulesets based on the devices you have selected.

View Jobs Associated with Rulesets

The **Jobs** page records actions when you apply ruleset to FDM-managed devices or remove them from FDM-managed devices. It also determines if the action was successful or failed.

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click a ruleset to view its details.

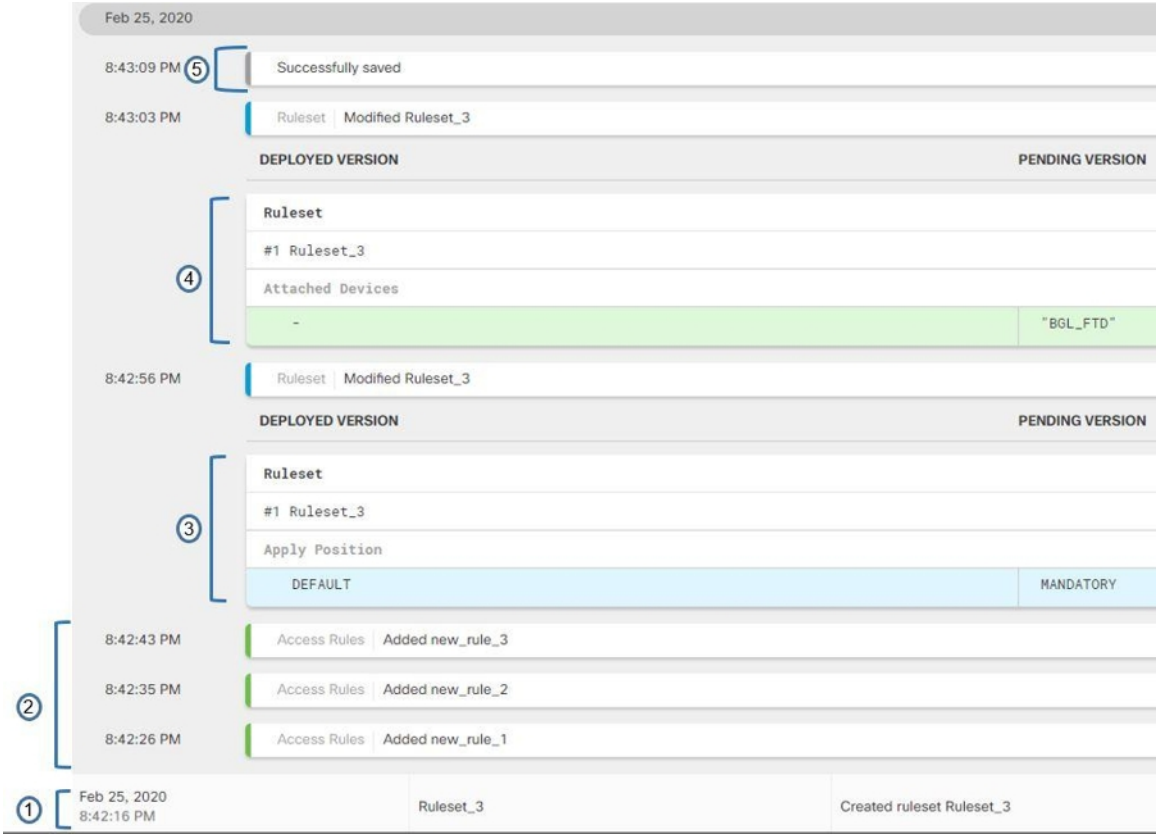
Step 3 In the **Management** pane, click **Jobs**. This page shows actions that you performed on the ruleset.

Change Log Entries after Creating Rulesets

When Security Cloud Control detects a change on the ruleset, it creates a change log entry for every action performed on the ruleset.

Clicking the blue View Change Log Differences link in the change log entry row displays a side-by-side comparison of the changes in the context of the running configuration file.

In the following example, the change log shows entries for a new ruleset with three rules added to the ruleset. It also shows information about setting the ruleset's priority and the FDM-managed device attached to the ruleset.



Number in Illustration	Explanation
1	The new ruleset "Ruleset_3" is created at 11:03:18 A.M on Feb 25, 2020.
2	The new access rules "new_rule_1", "new_rule_3", and "new_rule_3" are created in the ruleset.
3	The ruleset's priority is set to "Mandatory".
4	The ruleset is attached to the "BGL_FTD" device.
5	The ruleset changes are saved.

Detach FDM-Managed Devices from a Selected Ruleset

Use the following procedure to detach devices from a ruleset:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Select the ruleset you want to edit and click the **Edit** link in the **Actions** pane.

Step 3 On the top right corner, click the **Device** button appearing beside **Ruleset for**.

Step 4 Uncheck the devices that are currently attached to the ruleset, or click **Clear** to remove all devices at once.

Step 5 Click **Save**.

Step 6 Click **Save** in the upper right window to save the ruleset. Saving the policy stages the changes to Security Cloud Control.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Rulesets
- Configure Rulesets for a Device
- Create Rulesets from Existing Device Rules
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Delete Rules and Rulesets

Delete Rules and Rulesets

Delete Rules from a Ruleset

You can delete a rule that you no longer need in the ruleset.

Use the following procedure to delete rules:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click **Edit** in the **Actions** pane.

Step 3 Select a rule that you want to delete and then click **Remove** under **Actions**.

Step 4 Click **OK** to confirm the deletion.

Step 5 Click **Save** in the upper right corner to save the changes made to the ruleset. Saving the ruleset stages the changes to Security Cloud Control.

Step 6 Preview and Deploy Configuration Changes for All Devices your changes now or wait and deploy multiple changes at one time.

Delete a Ruleset

You can delete a ruleset only after detaching all devices associated with it. See Delete Rules and Rulesets.

Use the following procedure to delete a ruleset:

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click **Remove** inside the ruleset row.

Step 3 Click **Confirm** to delete the ruleset permanently.

Step 4 Preview and Deploy Configuration Changes for All Devices your changes now or wait and deploy multiple changes at one time.

- Rulesets
- Configure Rulesets for a Device
- Detach FDM-Managed Devices from a Selected Ruleset

Remove a Ruleset From a Selected FDM-Managed Device

There are two ways of removing a ruleset from a selected FDM-managed device, but their behaviors are slightly different.

- Delete a Ruleset From a Selected FDM-Managed Device: This feature deletes a Ruleset and its associated shared rules from a selected FDM-managed device.
- Disassociate a Ruleset From a Selected FDM-Managed Device: This feature doesn't remove the shared rules. Instead, it converts the shared rules to local rules.

Delete a Ruleset From a Selected FDM-Managed Device

You can delete a ruleset and its associated shared rules from a selected FDM-managed device. The ruleset can also be Detach FDM-Managed Devices from a Selected Ruleset from the ruleset page.

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 Click the delete icon appearing on the top right corner of a ruleset.

Step 5 Click **Confirm**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Disassociate a Ruleset From a Selected FDM-Managed Device

If you want to add a new device-specific rule to a ruleset in an FDM-managed device, you need to dissociate that ruleset from the FDM-managed device, which converts its associated shared rules to local rules. Then, you can add the rules that you want to local rules.

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Click the icon appearing on the top right corner of a ruleset.

Step 6 Click **Confirm**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Adding Comments to Rules in Policies and Rulesets

You can add comments to rules in FDM-managed device policies and rules in rulesets to document some characteristic of a rule. Rule comments are are only visible on Security Cloud Control; they are never written to the FDM-managed device nor are they visible in FDM.

Comments are added to rules after they are created and saved in Security Cloud Control. As rule comments are only a feature of Security Cloud Control, creating, changing, or deleting a rule comment does not change the configuration status of the device in Security Cloud Control to "Not Synced". You will not need to write changes from Security Cloud Control to the FDM-managed device to save a rule comment.

Comments associated with rules in an FDM-managed device policy can be viewed and edited on the device's policy page. Comments associated with rules in an FDM-managed device ruleset can be viewed and edited on the rulesets page. When a ruleset is used in a policy, any comments associated with any of the rules in the ruleset are displayed in the comments area of the policy. The comments are read-only.

When you search for a string in policies, rulesets, or the change log, Security Cloud Control will search the comments associated with a rule for that string along with the other attributes and values of a rule.

When a comment for a rule is added or edited, that action is recorded in the Change log. Because rule comments are only recorded and maintained in Security Cloud Control, they are labeled (Security Cloud Control-only change) in the change log.

Caution If there is an out of band change to an FDM-managed device's configuration and Security Cloud Control reads that configuration into its database, the comments associated with any rules will be wiped out.

Adding a Comment to a Rule

Procedure

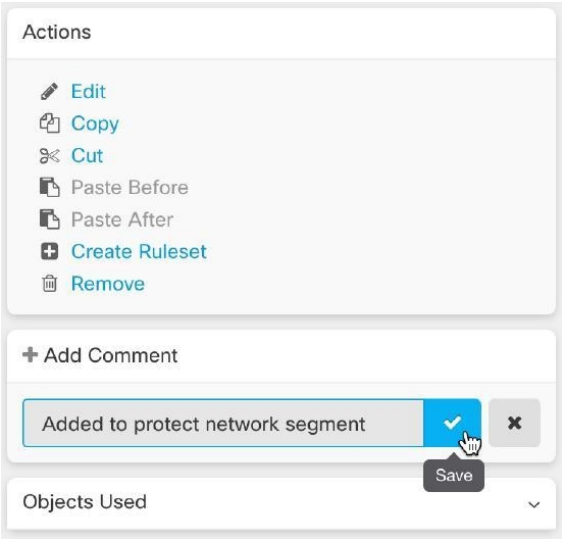
Step 1 Open the policy or ruleset that contains the rule you want to comment on.

Step 2 Select the rule.

Step 3 Click **Add Comment** in the Add Comment area for the rule.

Step 4 Add a comment in the text box.

Step 5 Click **Save**.



Editing Comments about Rules in Policies and Rulesets

Editing a comment on a rule in a policy

Use this procedure to edit a comment on a rule in an FDM-managed device policy.

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**.

Step 2 Select the FDM-managed device policy with the Local Rule you are going to add a comment to. You are not able to add a comment to a rule in a ruleset within a policy.

Step 3 In the Comment pane, click the edit icon .

Step 4 Edit the comment and click save. You will see the comment change reflected in the Comment area immediately.

Editing a comment on a rule in a ruleset

In order to see a change to a comment on a rule in a ruleset, reflected on the policy page, you have to make changes to the comment and the rule in a specific order.

Procedure

Step 1 In the left pane, click **Policies** > **FDM** > **Rulesets**.

Step 2 Select the ruleset with the rule you want to add a comment to.

Step 3 In the Actions pane, click **Edit**.

Step 4 Select the rule.

Step 5 In the Comment pane, click the edit icon  .

Step 6 Edit the comment and click save. You will see the comment change reflected in the Comment area of the ruleset page immediately.

Step 7 Select the rule you are going to change and in the Actions pane, click **Edit**.

Step 8 Edit the rule and click the blue check button to save the change.

Step 9 At the top of the ruleset page, click **Save** to save the ruleset. The new comment for the rule in the ruleset will now be reflected on a policy page.

Step 10 To see the comment change in a policy page:

a) From the Security Cloud Control menu bar, select **Policies > FTD/Meraki/AWS Policies**.

b) Select an FDM-managed device policy that contains the ruleset you just edited.

c) Select the rule with the comment you just edited. You should see your new comment in the Comment pane.

Network Address Translation

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private and not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of Network Address Translation (NAT) is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security-Keeping internal IP addresses hidden discourages direct attacks.

- IP routing solutions-Overlapping IP addresses are not a problem when you use NAT.
- Flexibility-You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.
- Translating between IPv4 and IPv6 (Routed mode only)-If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

You can use Security Cloud Control to create NAT rules for many different use cases. Use the NAT rule wizard or these topics to create different NAT rules:

Order of Processing NAT Rules

Network Object NAT and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Table 15: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Twice NAT (ASA) Manual NAT (FTD)	Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, twice NAT rules are added to section 1.
Section 2	Network Object NAT (ASA) Auto NAT (FTD)	If a match in section 1 is not found, section 2 rules are applied in the following order: **1.** Static rules. **2.** Dynamic rules. **Within each rule type, the following ordering guidelines are used:** **1.** Quantity of real IP addressesâ€”From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. **2.** For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. **3.** If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, object "Arlington" is assessed before object "Detroit."

Table Section	Rule Type	Order of Rules within the Section
Section 3	Twice NAT (ASA) Manual NAT (FTD)	If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 172.16.1.0/24 (dynamic) (object Arlington)

The resultant ordering would be:

- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object Arlington)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 192.168.1.0/24 (dynamic)

Network Address Translation Wizard

The Network Address Translation (NAT) wizard helps you create NAT rules on your devices for these types of access:

- **Enable Internet Access for Internal Users**. You may use this NAT rule to allow users on an internal network to reach the internet.
- **Expose an Internal Server to the Internet**. You may use this NAT rule to allow people outside your network to reach an internal web or email server.

Prerequisites to "Enable Internet Access for Internal Users"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.

- If you want to allow only specific users to reach the internet, you need the subnet addresses for those users.

Prerequisites to "Expose an Internal Server to the Internet"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- The IP address of the server inside your network that you would like to translate to an internet-facing IP address.
- The public IP address you want the server to use.

What to do Next

See Create a NAT Rule by using the NAT Wizard, on page 410.

Create a NAT Rule by using the NAT Wizard

Before you begin

See Network Address Translation Wizard, on page 409 for the prerequisites needed to create NAT rules using the NAT wizard.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Use the Filters and Page Level Search fields to find the device for which you want to create the NAT rule.

Step 5 In the **Management** area of the details panel, click **NAT** NAT.

Step 6 Click + > **NAT Wizard**.

Step 7 Respond to the NAT Wizard questions and follow the on-screen instructions.

- The NAT Wizard creates rules with Network Objects, on page 118. Either select an existing object from the drop-down menu, or create a new object with the create button + Create... .
- Before you can save the NAT rule, all IP addresses need to be defined as network objects.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Common Use Cases for NAT

Twice NAT and Manual NAT

Here are some common tasks that can be achieved using "Network Object NAT", also known as "Auto NAT":

- Enable a Server on the Inside Network to Reach the Internet Using a Public IP address, on page 411
- Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address, on page 412
- Make a Server on the Inside Network Available on a Specific Port of a Public IP Address, on page 413
- Translate a Range of Private IP Addresses to a Range of Public IP Addresses, on page 416

Network Object NAT and Auto NAT

Here is a common task that can be achieved using "Twice NAT", also know as "Manual NAT":

- Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface, on page 417

Enable a Server on the Inside Network to Reach the Internet Using a Public IP address

Use Case

Use this NAT strategy when you have a server with a private IP address that needs to be accessed from the internet and you have enough public IP addresses to NAT one public IP address to the private IP address. If you have a limited number of public IP addresses, see Make a Server on the Inside Network Available on a Specific Port of a Public IP Address (that solution may be more suitable).

Strategy

Your server has a static, private IP address, and users outside your network have to be able to reach your server. Create a network object NAT rule that translates the static private IP address to a static public IP address. After that, create an access policy that allows traffic from that public IP address to reach the private IP address. Finally, deploy these changes to your device.

Before you begin

Before you begin, create two network objects. Name one object *servername*_inside and the other object *servername*_outside. The *servername*_inside network object should contain the private IP address of your server. The *servername*_outside network object should contain the public IP address of your server. See Network Objects for instructions.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

a. Expand the Original Address menu, click **Choose**, and select the **servername_inside** object.

b. Expand the Translated Address menu, click **Choose**, and select the **servername_outside** object.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 For ASA, deploy a Network Policy rule or for FDM-managed device, deploy an access control policy rule to allow the traffic to flow from *servername*_inside to *servername*_outside.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address

Use Case

Allow users and computers in your private network to connect to the internet by sharing the public address of your outside interface.

Strategy

Create a port address translation (PAT) rule that allows all the users on your private network to share the outside interface public IP address of your device.

After the private address is mapped to the public address and port number, the device records that mapping. When incoming traffic bound for that public IP address and port is received, the device sends it back to the private IP address that requested it.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  **Network Object NAT.**

Step 7 In section 1, **Type**, select **Dynamic.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **any** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions :

a. Expand the Original Address menu, click **Choose** and select the **any-ipv4** or **any-ipv6** object depending on your network configuration.

b. Expand the Translated Address menu, and select **interface** from the available list. Interface indicates to use the public address of the outside interface.

Step 10 For an FDM-managed device, in section 5, **Name**, enter a name for the NAT rule.

Step 11 Click **Save**.

Step 12 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

NAT rules created by this procedure:

```
object network any_network
nat (any,outside) dynamic interface
```

Make a Server on the Inside Network Available on a Specific Port of a Public IP Address

Use Case

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Prerequisites

Before you begin, create three separate network objects, one each for an FTP, HTTP, and SMTP server. For the sake of the following procedures, we call these objects **ftp-server-object**, **http-server-object**, and **smtp-server-object**. See Create or Edit a Firepower Network Object or Network Groups for instructions.

NAT Incoming FTP Traffic to an FTP Server

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **ftp**-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **ftp, ftp.**

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

NAT Incoming HTTP Traffic to an HTTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the http server. For the sake of this procedure, we will call the object, **http-object**. See Create or Edit a Firepower Network Object or Network Groups for instructions.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **http**-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **http**, http.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

NAT Incoming SMTP Traffic to an SMTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the smtp server. For the sake of this procedure, we will call the object, **smtp-object**. See Create or Edit a Firepower Network Object or Network Groups for instructions.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the smtp-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **smtp**, **smtp.**

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Translate a Range of Private IP Addresses to a Range of Public IP Addresses

Use Case

Use this approach if you have a group of specific device types, or user types, that need to have their IP addresses translated to a specific range so that the receiving devices (the devices on the other end of the transaction) allow the traffic in.

Translate a Pool of Inside Addresses to a Pool of Outside Addresses

Before you begin

Create a network object for the pool of private IP addresses you want to translate and create a network object for the pool of public addresses you want to translate those private IP addresses into.

Note For the ASA FTD, the network group that defines the pool of "translated address" cannot be a network object that defines a subnet.

When creating these address pools, use Create or Edit a Firepower Network Object or Network Groups for instructions.

For the sake of the following procedure, we named the pool of private addresses, **inside_pool** and name the pool of public addresses, **outside_pool.**

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT**.

Step 7 In section 1, **Type**, select **Dynamic** and click **Continue**.

Step 8 In section 2, **Interfaces**, set the source interface to **inside** and the destination interface to **outside**. Click **Continue**.

Step 9 In section 3, **Packets**, perform these tasks:

- For the Original Address, click **Choose** and then select the **inside_pool** network object (or network group) you made in the prerequisites section above.
- For the Translated Address, click **Choose** and then select the **outside_pool** network object (or network group) you made in the prerequisites section above.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface

Use Case

Use this Twice NAT use case to enable site-to-site VPN.

Strategy

You are translating a pool of IP addresses to itself so that the IP addresses in one location on the network arrives unchanged in another.

Create a Twice NAT Rule

Before you begin

Create a network object or network group that defines the pool of IP addresses you are going to translate to itself. For the ASA, the range of addresses can be defined by a network object that uses an IP address range, a network object that defines a subnet, or a network group object that includes all the addresses in the range. For the FTD, the range of addresses can be defined by a network object that defines a subnet or a network group object that includes all the addresses in the range.

When creating the network objects or network groups, use Create or Edit a Firepower Network Object or Network Groups for instructions.

For the sake of the following procedure, we are going call the network object or network group, Site-to-Site-PC-Pool.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Twice NAT.**.

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, make these changes:

- Expand the Original Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.
- Expand the Translated Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 For an ASA, create a crypto map. See CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide and review the chapter on LAN-to-LAN IPsec VPNs for more information on creating a crypto map.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Manage Virtual Private Network Management in Security Cloud Control

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet.

This section applies to Remote Access and Site-to-site VPNs on FDM-managed device. It describes the Internet Protocol Security (IPsec) standards to build site-to-site VPNs connection on FTD. It also describes the SSL standards that are used to build and remote access VPN connections on FTD.

Security Cloud Control supports the following types of VPN connections:

- Introduction to Site-to-Site Virtual Private Network, on page 419
- Introduction to Remote Access Virtual Private Network

For additional information about Virtual Private Networks, refer to the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Introduction to Site-to-Site Virtual Private Network

A site-to-site VPN tunnel connects networks in different geographic locations. You can create site-to-site IPsec connections between managed devices and between managed devices and other Cisco or third-party peers that comply with all relevant standards. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and Internet Key Exchange version 2 (IKEv2). After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

VPN Topology

To create a new site-to-site VPN topology you must provide a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both and authentication method. Once configured, you deploy the topology to FTD.

IPsec and IKE Protocols

In Security Cloud Control, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

Authentication VPN Tunnels

For authentication of VPN connections, configure a pre-shared key in the topology on each device. Pre-shared keys allow a secret key, used during the IKE authentication phase, to be shared between two peers.

Virtual Tunnel Interface (VTI)

Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on FTD. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores the VTI interfaces. If a security zone or static route references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference.

About Extranet Devices

You can add non-Cisco or unmanaged Cisco devices to a VPN topology as "Extranet" devices with either static or dynamic IP addresses.

- Non-Cisco Device: You cannot use Security Cloud Control to create and deploy configurations to non-Cisco devices.

- Unmanaged Cisco Device: Cisco device not managed by your organization, such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.

Related Information:

- Configure Site-to-Site VPN for an FDM-Managed Device, on page 420
- Monitor FDM-Managed Device Site-to-Site Virtual Private Networks

Configure Site-to-Site VPN for an FDM-Managed Device

Security Cloud Control supports these aspects of site-to-site VPN functionality on FDM-managed devices:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual pre-shared keys for authentication.
- IPv4 and IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 site-to-site VPN topologies provide configuration settings to comply with Security Certifications.
- Static and dynamic interfaces.
- Support for the dynamic IP address for the extranet device as an endpoint.

Configure Site-to-Site VPN Connections with Dynamically Addressed Peers

Security Cloud Control allows you to create a site-to-site VPN connection between peers when one of the peers' VPN interface IP address is not known or when the interface obtains its address from a DHCP server. Any dynamic peer whose preshared key, IKE settings, and IPsec configurations match with another peer can establish a site-to-site VPN connection.

Consider two peers, A and B. The static peer is a device whose IP address of its VPN interface is fixed and a dynamic peer is a device whose IP address of the VPN interface is not known or has a temporary IP address.

The following use cases describe different scenarios for establishing a secure site-to-site VPN connection with dynamically-addressed peers:

- A is a static peer, and B is a dynamic peer or conversely.
- A is a static peer, and B is a dynamic peer with a resolved IP address from the DHCP server or conversely. You can select **Bind VPN to the assigned IP** to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.
- A and B are dynamic with resolved IP addresses from the DHCP server. In such a case, you must select **Bind VPN to the assigned IP** for at least one peer to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.
- A is a dynamic peer, and B is an extranet device with a static or dynamic IP address.
- A is a dynamic peer with a resolved IP address from the DHCP server, and B is an Extranet device with a static or dynamic IP address. You can select **Bind VPN to the assigned IP** to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.

Important If you select **Bind VPN to the assigned IP**, the VPN binds statically to the DHCP assigned IP address. However, this dynamic interface can receive many new IP addresses after the peer restarts. Although the VPN tunnel updates the new IP address, the other peer is not updated with the new configuration. You must deploy the site-to-site configuration again for out-of-band changes on the other peer.

Note If the IP address of the interface is changed by using a local manager like firewall device manager, the **Configuration Status** of that peer in Security Cloud Control shows "Conflict Detected". When you Resolve Configuration Conflicts, the **Configuration Status** of the other peer changes to the "Not Synced" state. You must deploy the Security Cloud Control configuration to the device which is in "Not Synced" state.

Typically, the dynamic peer must be the one that initiates the connection as the other peer would not know the IP address of the dynamic peer. When the remote peer attempts to establish the connection, the other peer validates the connection using the preshared key, IKE settings, and IPsec configurations.

Because the VPN connection is established only after the remote peer initiates the connection, any outbound traffic that matches access control rules that allow traffic in the VPN tunnel will be dropped until that connection is established. This ensures that data does not leave your network without the appropriate encryption and VPN protection.

Note A site-to-site VPN connection cannot be configured in the following scenarios:

- If both peers have DHCP assigned IP addresses.
  - **Workaround**: You can configure a site-to-site VPN, if one of the peers has a resolved IP address from the DHCP server. In such a case, you must select **Bind VPN to the assigned IP** to configure site-to-site VPN.
- If a device has more than one dynamic peer connection.
  - **Workaround**: You can configure a site-to-site VPN by performing the following steps:
    - Consider three devices A, B, and C.
    - Configure site-to-site VPN connection between A (static peer) and B (dynamic peer).
    - Configure site-to-site VPN connection between A and C (dynamic peer) by creating an Extranet device. Assign the static VPN interface IP address of A to the Extranet device and establish a connection with C.

FDM-Managed Device Site-to-Site VPN Guidelines and Limitations

- Security Cloud Control does not support a crypto-acl to design the interesting traffic for S2S VPN. It only supports protected networks.
- Security Cloud Control does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control but it ignores the VTI interfaces. If a security zone or static route

references a VTI, Security Cloud Control reads the security zone and static route without the VTI reference. Security Cloud Control support for VTI tunnels is coming soon.

- Whenever IKE ports 500/4500 are in use or when there are some PAT translations that are active, the site-to-site VPN cannot be configured on the same ports as it fails to start the service on those ports.
- Transport mode is not supported only tunnel mode. IPsec tunnel mode encrypts the entire original IP datagram which becomes the payload in a new IP packet. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind a firewall. Tunnel mode is the normal way regular IPsec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- For this release, only PTP topology is supported, containing one or more VPN tunnels. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Related Information:

- Create a Site-To-Site VPN
- Edit an Existing Security Cloud Control Site-To-Site VPN
- Encryption and Hash Algorithms Used in VPN
- Exempt Site-to-Site VPN Traffic from NAT

Encryption and Hash Algorithms Used in VPN

Because a VPN tunnel typically traverses a public network, most likely the Internet, you need to encrypt the connection to protect the traffic. You define the encryption and other security techniques to apply using IKE policies and IPsec proposals.

If your device license allows you to apply strong encryption, there is a wide range of encryption and hash algorithms, and Diffie-Hellman groups, from which to choose. However, as a general rule, the stronger the encryption that you apply to the tunnel, the worse the system performance. Find a balance between security and performance that provides sufficient protection without compromising efficiency.

We cannot provide specific guidance on which options to choose. If you operate within a larger corporation or other organization, there might already be defined standards that you need to meet. If not, take the time to research the options.

The following topics explain the available options:

Deciding Which Encryption Algorithm to Use

When determining which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN.

For IKEv2, you can configure multiple encryption algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

For IPsec proposals, the algorithm is used by the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP.

If your device license qualifies for strong encryption, you can choose from the following encryption algorithms. If you are not qualified for strong encryption, you can select DES only.

- AES-GCM - (IKEv2 only.) Advanced Encryption Standard in Galois/Counter Mode is a block cipher mode of operation providing confidentiality and data-origin authentication and provides greater security than AES. AES-GCM offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance. GCM is a mode of AES that is required to support NSA Suite B. NSA Suite B is a set of cryptographic algorithms that devices must support to meet federal standards for cryptographic strength.
- AES-GMAC - (IKEv2 IPsec proposals only.) Advanced Encryption Standard Galois Message Authentication Code is a block cipher mode of operation providing only data-origin authentication. It is a variant of AES-GCM that allows data authentication without encrypting the data. AES-GMAC offers three different key strengths: 128-, 192-, and 256-bit keys.
- AES - Advanced Encryption Standard is a symmetric cipher algorithm that provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance.
- DES - Data Encryption Standard, which encrypts using 56-bit keys, is a symmetric secret-key block algorithm. If your license account does not meet the requirements for export controls, this is your only option. It is faster than 3DES and uses fewer system resources, but it is also less secure. If you do not need strong data confidentiality, and if system resources or speed is a concern, choose DES.
- 3DES - Triple DES, which encrypts three times using 56-bit keys, is more secure than DES because it processes each block of data three times with a different key. However, it uses more system resources and is slower than DES.
- NULL - A null encryption algorithm provides authentication without encryption. This is typically used for testing purposes only.

Deciding Which Hash Algorithms to Use

In IKE policies, the hash algorithm creates a message digest, which is used to ensure message integrity. In IKEv2, the hash algorithm is separated into two options, one for the integrity algorithm, and one for the pseudo-random function (PRF).

In IPsec proposals, the hash algorithm is used by the Encapsulating Security Protocol (ESP) for authentication. In IKEv2 IPsec Proposals, this is called the integrity hash. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-, and there is also an -HMAC suffix (which stands for "hash method authentication code").

For IKEv2, you can configure multiple hash algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

You can choose from the following hash algorithms:

- SHA (Secure Hash Algorithm) - Standard SHA (SHA-1) produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. However, it is also more resource-intensive than MD5. For implementations that require the highest level of security, use the SHA hash algorithm.
- The following SHA-2 options, which are even more secure, are available for IKEv2 configurations. Choose one of these if you want to implement the NSA Suite B cryptography specification.
  - SHA-256 - Specifies the Secure Hash Algorithm SHA-2 with the 256-bit digest.
  - SHA-384 - Specifies the Secure Hash Algorithm SHA-2 with the 384-bit digest.
  - SHA-512 - Specifies the Secure Hash Algorithm SHA-2 with the 512-bit digest.

- MD5 (Message Digest 5) - Produces a 128-bit digest. MD5 uses less processing time for overall faster performance than SHA, but it is considered to be weaker than SHA.
- Null or None (NULL, ESP-NONE) - (IPsec Proposals only.) A null Hash Algorithm; this is typically used for testing purposes only. However, you should choose the null integrity algorithm if you select one of the AES-GCM/GMAC options as the encryption algorithm. Even if you choose a non-null option, the integrity hash is ignored for these encryption standards.

Deciding Which Diffie-Hellman Modulus Group to Use

You can use the following Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has different size modules. A larger modulus provides higher security but requires more processing time. You must have a matching modulus group on both peers.

If you select AES encryption, to support the large key sizes required by AES, you should use Diffie-Hellman (DH) Group 5 or higher. IKEv1 policies do not support all of the groups listed below.

To implement the NSA Suite B cryptography specification, use IKEv2 and select one of the elliptic curves Diffie-Hellman (ECDH) options: 19, 20, or 21. Elliptic curve options and groups that use 2048-bit modulus are less exposed to attacks such as Logjam.

For IKEv2, you can configure multiple groups. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

- 2 - Diffie-Hellman Group 2: 1024-bit modular exponential (MODP) group. This option is no longer considered good protection.
- 5 - Diffie-Hellman Group 5: 1536-bit MODP group. Formerly considered good protection for 128-bit keys, this option is no longer considered good protection.
- 14 - Diffie-Hellman Group 14: 2048-bit modular exponential (MODP) group. Considered good protection for 192-bit keys.
- 19 - Diffie-Hellman Group 19: National Institute of Standards and Technology (NIST) 256-bit elliptic curve modulo a prime (ECP) group.
- 20 - Diffie-Hellman Group 20: NIST 384-bit ECP group.
- 21 - Diffie-Hellman Group 21: NIST 521-bit ECP group.
- 24 - Diffie-Hellman Group 24: 2048-bit MODP group with 256-bit prime order subgroup. This option is no longer recommended.

Deciding Which Authentication Method to Use

You can use the following methods to authenticate the peers in a site-to-site VPN connection.

Preshared Keys

Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase. For IKEv1, you must configure the same preshared key on each peer. For IKEv2, you can configure unique keys on each peer.

Preshared keys do not scale well compared to certificates. If you need to configure a large number of site-to-site VPN connections, use the certificate method instead of the preshared key method.

Create a Site-To-Site VPN

You can create a site-to-site VPN by following one of the two methods: simple configuration and advanced configuration. In a simple configuration, the default configuration is used for establishing the site-to-site VPN connection. You can modify the configuration in the **Advanced** mode.

Each site-to-site VPN topology can include extranet devices that you do not manage in Security Cloud Control. An Extranet device can be any device (Cisco or third-party), which is not managed by Security Cloud Control.

For this release, only PTP topology is supported, containing one tunnel per site-to-site connection. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Related information:

- Create a Site-To-Site VPN using the Simple Configuration, on page 425
- Create a Site-To-Site VPN using the Advanced Configuration, on page 426
- Configure Networking for Protected Traffic Between the Site-To-Site Peers, on page 428

Create a Site-To-Site VPN using the Simple Configuration

Procedure

Step 1 In the left pane, choose **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

Step 2 Click the blue plus button to create a VPN Tunnel.

Note Alternatively, you can create the Site-to-Site VPN connection from the **Inventory** page.

a. On the navigation bar, click **Inventory**.

b. Select two FDM-managed devices that you want to configure. If you select an extranet device, specify the extranet device's IP address.

c. In the right-page, under **Device Actions,** click **Create Site-to-Site VPN**.

Step 3 Enter a unique topology **Configuration Name**. We recommend naming your topology to indicate that it is an FDM-managed device VPN, and its topology type.

Step 4 Choose the endpoint devices for this VPN deployment from Devices.

Step 5 If you choose an extranet device in **Peer 2**, select **Static,** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.

Step 6 Choose the **VPN Access Interface** for the for the endpoint devices.

Note If one or both endpoint devices have dynamic IP addresses, see Configure Site-to-Site VPN Connections with Dynamically Addressed Peers for additional instructions.

Step 7 Click the blue plus button to add the **Protected Networks** for the participating devices.

Step 8 (Optional) Select **NAT Exempt** to exempt the VPN traffic from NAT policies on the local VPN access interface. It must be configured manually for individual peers. If you do not want NAT rules to apply to the local network, select the interface that hosts the local network. This option works only if the local network

resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface or one or more bridge group members, you must manually create the NAT exempt rules. For information on manually creating the required rules, see Exempt Site-to-Site VPN Traffic from NAT .

Step 9 Click **Create VPN**, and then click **Finish**.

Step 10 Perform the additional mandatory configuration. See Configure Networking for Protected Traffic Between the Site-To-Site Peers.

The Site-To-Site VPN is configured.

Create a Site-To-Site VPN using the Advanced Configuration

Procedure

Step 1 In the left pane, choose **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

Step 2 Click the blue plus  button to create a VPN Tunnel.

Step 3 In the **Peer Devices** section, specify the following device configurations:

a. Enter a unique topology **Configuration Name**. We recommend naming your topology to indicate that it is an FDM-managed devicee VPN, and its topology type.

b. Choose the endpoint devices for this VPN deployment from Devices.

c. If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.

d. Choose the **VPN Access Interface** for the endpoint devices.

Note If one or both endpoint devices have dynamic IP addresses, see Configure Site-to-Site VPN Connections with Dynamically Addressed Peers for additional instructions.

Step 4 Click the blue plus  button to add the **Protected Networks** for the participating devices.

Step 5 Click **Advanced**.

Step 6 In the **IKE Settings** section, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see the About Global IKE Policies, on page 144.

Note IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

a. Select either or both options as appropriate.

Note By default, **IKEV Version 2** is enabled and the **IKEV2 POLICIES**.

b. Click the blue plus  button and select the IKEv2 policies.

Click **Create New IKEv2 Policy** to create new IKEv2 policies. Alternatively, in Security Cloud Control click **Objects > FDM Objects**, then click > **IKEv2 Policy**. For more information about creating new IKEv2 policies, see the Managing IKEv2 Policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the **x** icon.

c. Click **IKE Version 1** to enable it.

d. Click the blue plus button and select the IKEv1 policies. Click **Create New IKEv1 Policy** to create new IKEv1 policies. Alternatively, you can go to the Security Cloud Control navigation bar and click **Objects > FDM Objects** , then click > **IKEv1 Policy**. For more information about creating new IKEv1 policies, see the Managing IKEv1 Policies. To delete an existing IKEv1 Policy, hover-over the selected policy and click the **x** icon.

e. Enter the **Pre-Shared Key** for the participating devices. Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase.

- (IKEv2) **Peer 1 Pre-shared Key**, **Peer 2 Pre-shared Key**: For IKEv2, you can configure unique keys on each peer. Enter the **Pre-shared Key**. You can click the **Show Override** button and enter the appropriate pre-shared for the peer. The key can be 1-127, alphanumeric characters. The following table describes the purpose of the pre-shared key for both peers.

	Local Pre-shared Key	Remote Peer Pre-shared Key
Peer 1	Peer 1 Pre-shared Key	Peer 2 Pre-shared Key
Peer 2	Peer 2 Pre-shared Key	Peer 1 Pre-shared Key

- (IKEv1) **Pre-shared Key**: For IKEv1, you must configure the same preshared key on each peer. The key can be 1-127, alphanumeric characters. In this scenario, Peer 1 and Peer 2 use the same pre-shared key to encrypt and decrypt data.

f. Click **Next**.

Step 7 In the **IPSec Settings** section, specify the IPSec configurations. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step.

For more information on the IPSec settings, see the About IPsec Proposals, on page 141.

a. Click the blue plus button and select the IKEv2 proposals. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the **x** icon.

Note Click Create New IKEv2 Proposal to create new IKEv2 proposals. Alternatively, you can go to the Security Cloud Control navigation bar and click **Objects > FDM Objects**, then click > **IKEv2 IPSec Proposal**.

For more information about creating new IKEv2 policies, see the Managing an IKEv2 IPsec Proposal Object.

b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Deciding Which Diffie-Hellman Modulus Group to Use.

c. Click **Create VPN**.

d. Read the configuration and then click **Finish** if you're satisfied.

e. Perform the additional mandatory configuration. See Configure Networking for Protected Traffic Between the Site-To-Site Peers.

Configure Networking for Protected Traffic Between the Site-To-Site Peers

After completing the configuring of the Site-To-Site connection, make sure that you perform the following configuration for VPN to function on all targeted devices.

Procedure

Step 1 Configure AC policies:

Configure AC policies for permitting bidirectional traffic between the protected networks behind both peers. These policies help the packets to traverse to the intended destination without being dropped.

Note You must create AC policies for incoming and outgoing traffic on both peers.

a. In the Security Cloud Control navigation bar at the left, click **Policies** and select the option that you want.

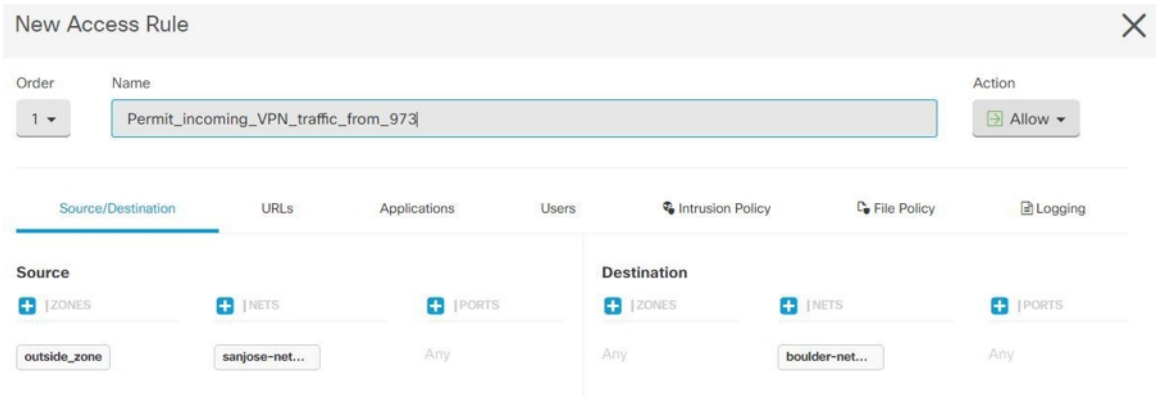
b. Create policies for incoming and outgoing traffic on both peers. For more information on AC policy creation, see Configure the FDM Access Control Policy.

The following example shows steps for creating AC policies on both peers.

Consider two FDM-managed devices 'FTD_BGL_972' and 'FTD_BGL_973' with Site-To-Site VPN connection between two protected networks 'boulder-network' and 'sanjose-network' respectively.

Creating the AC policy for permitting incoming traffic:

The policy 'Permit_incoming_VPN_traffic_from_973' is created on the 'FTD_BGL_972' device for allowing incoming traffic from the peer ('FTD_BGL_973').

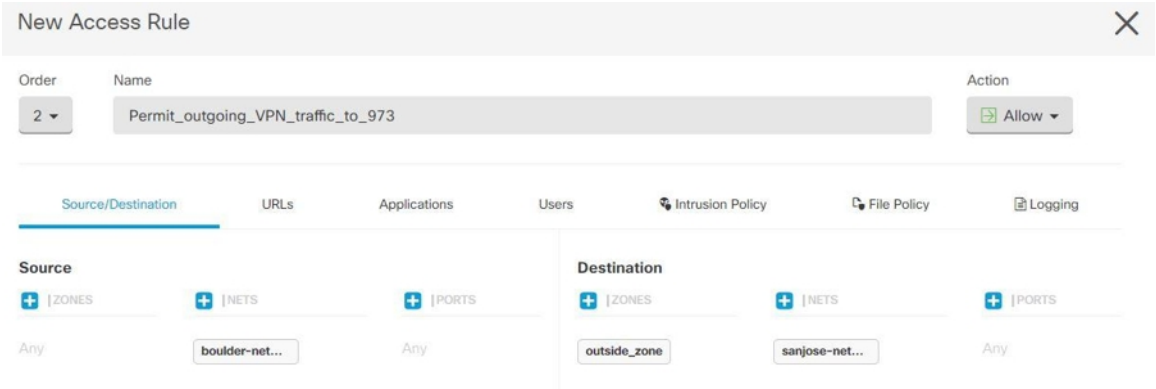


- **Source Zone**: Set the zone of the peer device from which the network traffic originates. In this example, the traffic is originating from FTD_BGL_973 and reaching FTD_BGL_972.

- **Source Network**: Set the protected network of the peer device from which the network traffic originates. In this example, traffic is originating from 'sanjose-network' which is the protected network behind the peer device (FTD_BGL_973).
- **Destination Network**: Set the protected network of the device on which the network traffic arrives. In this example, traffic is arriving at 'boulder-network' which is the protected network behind the peer device (FTD_BGL_972). **Note**: The remaining fields can have the default value ("Any").
- Set **Action** to **Allow** for allowing the traffic subject to the intrusion and other inspection settings in the policy.

Creating the AC policy for permitting outgoing traffic:

The policy 'Permit_outgoing_VPN_traffic_to_973' is created on the 'FTD_BGL_972' device for permitting outgoing traffic to the peer ('FTD_BGL_973').



- **Source Network**: Set the protected network of the peer device from which the network traffic originates. In this example, traffic is originating from 'boulder-network' which is the protected network behind the peer device (FTD_BGL_972).
- **Destination Zone**: Set the zone of the peer device on which the network traffic arrives. In this example, the traffic is arriving from FTD_BGL_972 and reaching FTD_BGL_973.
- **Destination Network**: Set the protected network of the peer on which the network traffic arrives. In this example, traffic is arriving on 'sanjose-network' which is the protected network behind the peer device (FTD_BGL_972). **Note**: The remaining fields can have the default value ("Any").
- Set **Action** to **Allow** for allowing the traffic subject to the intrusion and other inspection settings in the policy.

After creating AC policies on one device, you must create similar policies on its peer.

Step 2 If NAT is configured on either of the peer devices, you need to configure the NAT exempt rules manually. See Exempt Site-to-Site VPN Traffic from NAT .

Step 3 Configure routing for receiving the return VPN traffic on each peer. For more information, see Configure Static and Default Routes for FDM-Managed Devices.

a. **Gateway**-Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.

b. **Interface**-Select the interface through which you want to send traffic. In this example, the traffic is sent through 'outside' interface.

c. **Destination Networks**-Select one or network objects, that identify the destination network. In this example, the destination is 'sanjose-network' which is behind peer (FTD_BGL_973).

After configuring routing settings on one device, you must configure similar settings on its peer.

Edit an Existing Security Cloud Control Site-To-Site VPN

The advanced configuration wizard is used by default to modify an existing site-to-site VPN configuration.

Procedure

Step 1 In the left pane, choose **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

Step 2 Select the desired site-to-site VPN tunnel that you want to edit.

Step 3 In the **Actions** pane, click **Edit**.

Note Alternatively, you can perform the following to edit the configuration:

a. Open the VPN page and click **Global View** button in the filter panel (for more information, see Search and Filter Site-to-Site VPN Tunnels).

The illustration of all site-to-site VPN tunnels available across all devices appears.

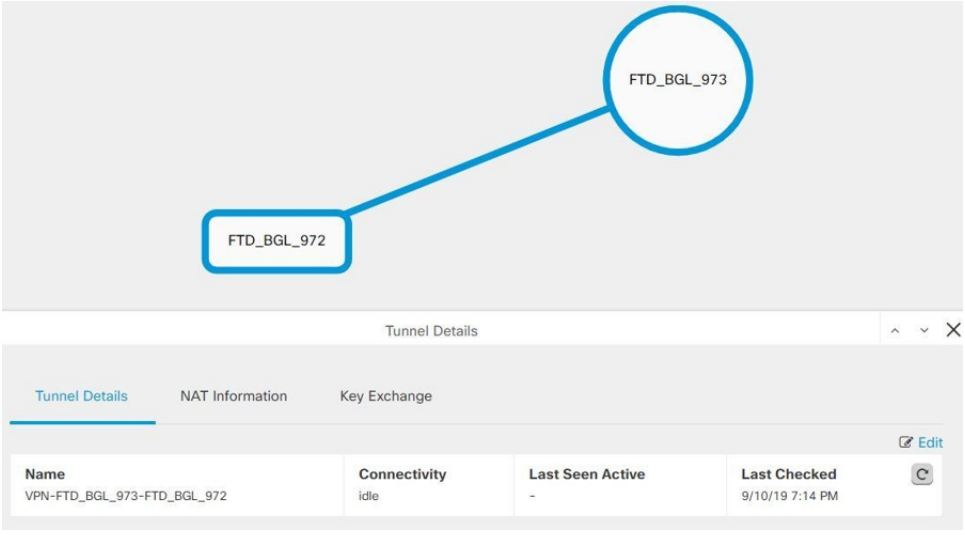
To edit the configuration, one of the peers must be FDM-managed device.

b. Select a device by clicking the box.

c. Click **View details** to view its peers.

d. Click the peer device to view the tunnel details.

You can view the tunnel details, NAT information, and key exchange information pertaining to the device.



e. Click **Edit** in **Tunnel Details**.

Step 4 In the **Peer Devices** section, you can modify the following device configurations: Configuration Name, VPN Access Interface, and Protected Networks.

Note You cannot change the participating devices.

Step 5 In the **IKE Settings** section, you can modify the following IKEv2 policies configurations:

a. Click the blue plus button for the respective device and select new IKEv2 policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the **x** icon.

b. Modify the **Pre-Shared Key** for the participating devices. If the pre-shared keys are different for endpoint devices, click the blue settings button and enter the appropriate pre-shared keys for the devices.

c. Click **Next**.

Step 6 In the **IPSec Settings** section, you can modify the following IPSec configurations:

a. Click the blue plus button to select new IKEv2 proposals. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the **x** icon.

b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**.

c. Click **Edit VPN**, and then **Finish**.

The Point to point VPN is modified and updated with all the changes you have made.

Delete a Security Cloud Control Site-To-Site VPN Tunnel

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select the desired site-to-site VPN tunnel that you want to delete.

Step 3 In the **Actions** pane on the right, click **Delete**.

The selected site-to-site VPN tunnel is deleted.

Exempt Site-to-Site VPN Traffic from NAT

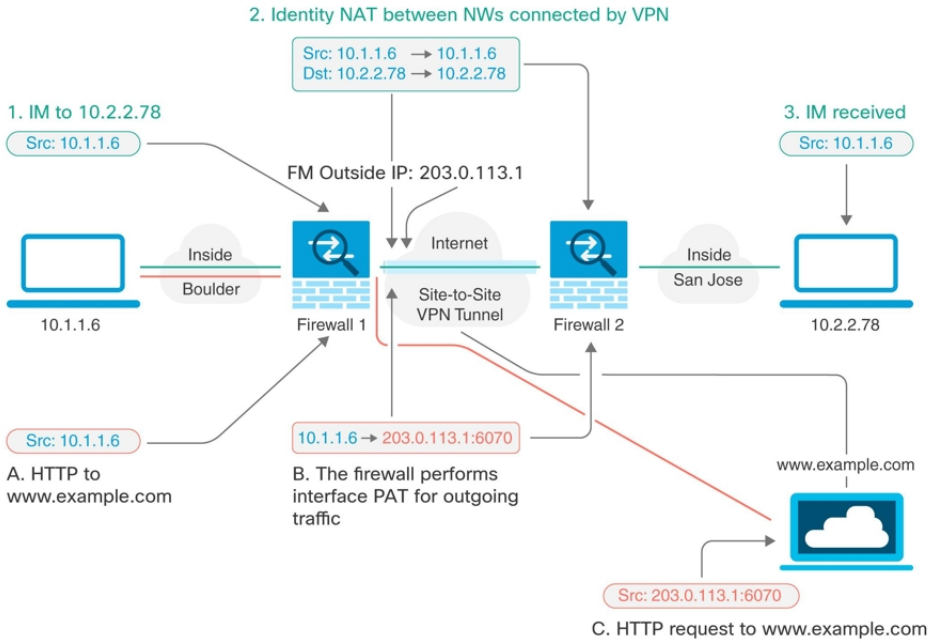
When you have a site-to-site VPN connection defined on an interface, and you also have NAT rules for that interface, you can optionally exempt the traffic on the VPN from the NAT rules. You might want to do this if the remote end of the VPN connection can handle your internal addresses.

When you create the VPN connection, you can select the **NAT Exempt** option to create the rules automatically. However, this works only if your local protected network is connected through a single routed interface (not a bridge group member). If instead, the local networks in the connection reside behind two or more routed interfaces or one or more bridge group members, you need to configure the NAT exempt rules manually.

To exempt VPN traffic from NAT rules, you create an identity manual NAT rule for the local traffic when the destination is the remote network. Then, apply NAT to the traffic when the destination is anything else (for example, the Internet). If you have more than one interface for the local network, create rules for each interface. Also, consider the following suggestions:

- If there is more than one local network in the connection, create a network object group to hold the objects that define the networks.
- If you are including both IPv4 and IPv6 networks in the VPN, create separate identity NAT rules for each.

Consider the following example, which shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface Port Address Translation (PAT) rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT translates an address to the same address.



The following example explains the configuration for Firewall1 (Boulder). The example assumes that the inside interface is a bridge group, so you need to write the rules for each member interface. The process is the same if you have a single or multiple routed inside interfaces.

Note This example assumes IPv4 only. If the VPN also includes IPv6 networks, create parallel rules for IPv6. Note that you cannot implement IPv6 interface PAT, so you need to create a host object with a unique IPv6 address to use for PAT.

Procedure

Step 1 Create objects to define the various networks.

a. In the left pane, click **Objects**.

b. Click the blue plus button to create an object.

c. Click **FTD** > **Network**.

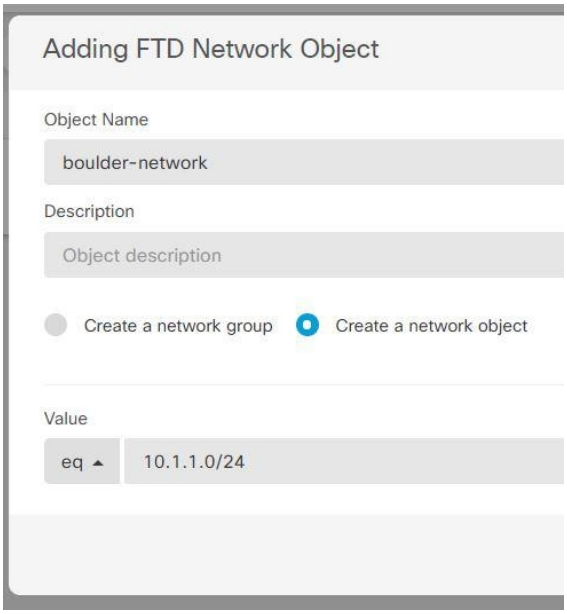
d. Identify the Boulder inside network.

e. Enter an object name (for example, boulder-network).

f. Select **Create a network object**.

g. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.



h. Click **Add**.

i. Click the blue plus button to create an object.

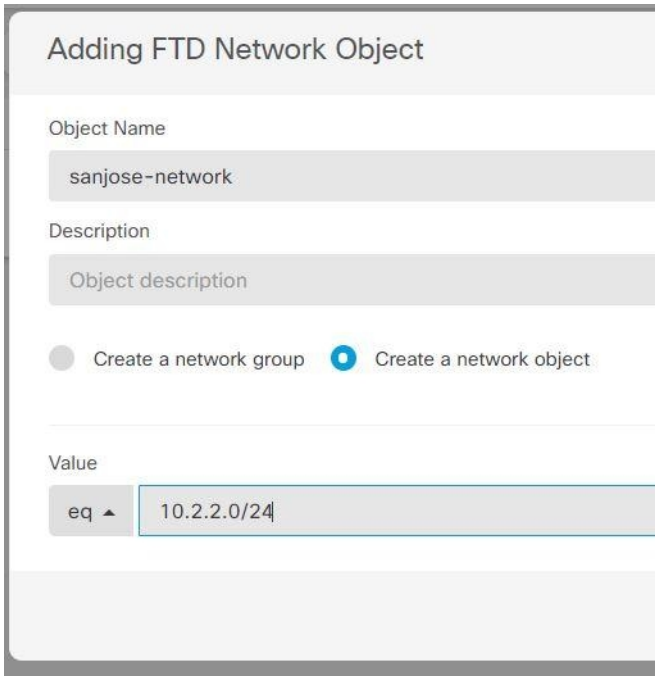
j. Define the inside San Jose network.

k. Enter the object name (for example, san-jose).

l. Select **Create a network object**.

m. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.



n. Click **Add**.

Step 2 Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

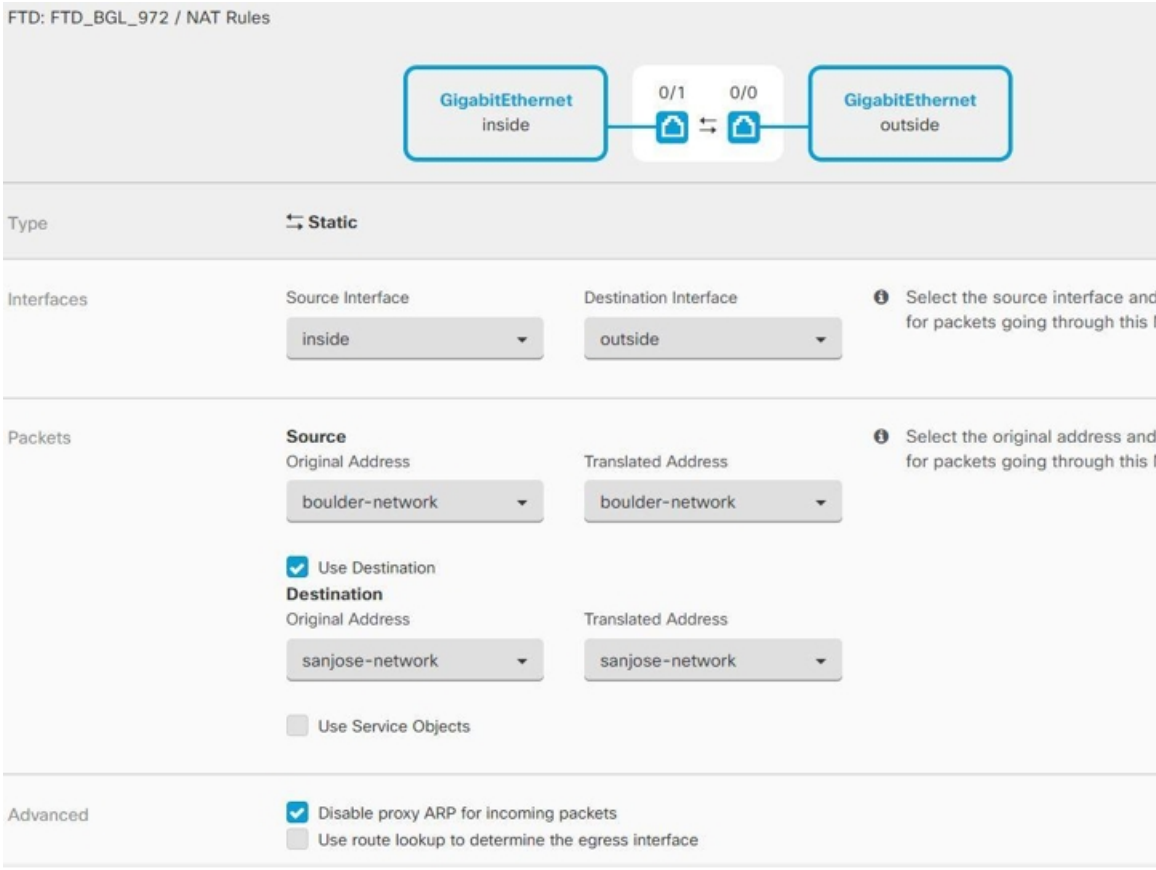
a. In the left pane, click **Security Devices** > **All Devices**.

b. Use the filter to find the device for which you want to create the NAT rule.

c. In the Management area of the details panel, click **NAT** NAT.

d. Click + > **Twice NAT**.

- In section 1, select **Static.** Click **Continue**.
- In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.
- In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'boulder-network'.
- Select **Use Destination**.
- Select **Destination Original Address** = 'sanjose-network' and **Source Translated Address** = 'sanjose-network'. **Note**: Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank. This rule configures identity NAT for both source and destination.



- Select **Disable proxy ARP for incoming packets**.
- Click **Save**.
- Repeat the process to create equivalent rules for each of the other inside interfaces.

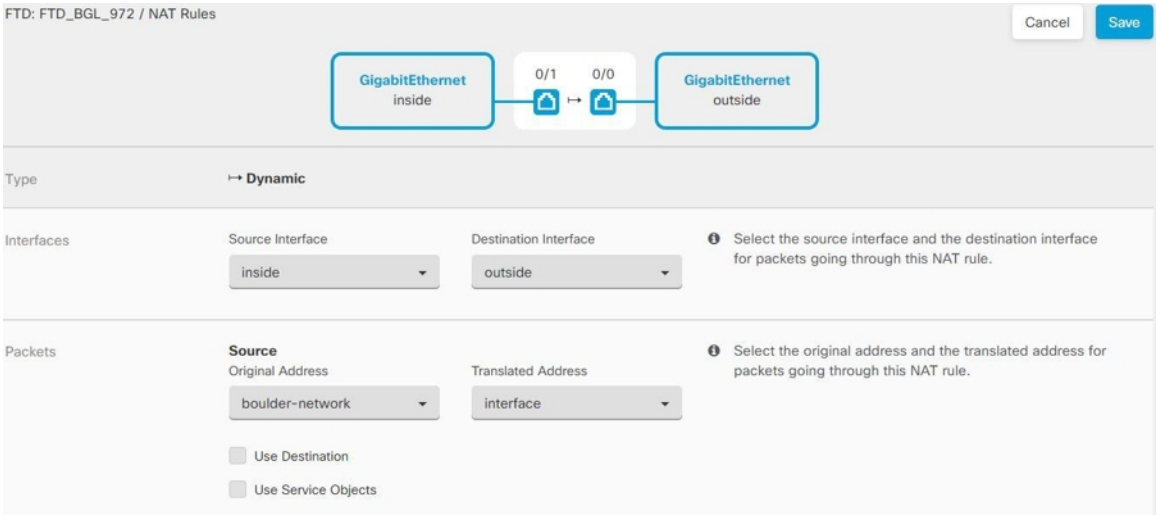
Step 3 Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder). **Note**: There might already be dynamic interface PAT rules for the inside interfaces, covering any IPv4 traffic, as these are created by default during initial configuration. However, the configuration is shown here for completeness. Before completing these steps, check whether a rule already exists that covers the inside interface and network, and skip this step if it does.

a. Click + > **Twice NAT**.

b. In section 1, select **Dynamic.** Click **Continue**.

c. In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.

d. In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'interface'.



e. Click **Save**.

f. Repeat the process to create equivalent rules for each of the other inside interfaces.

Step 4 Deploy configuration changes to Security Cloud Control. For more information, see Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device.

Step 5 If you are also managing Firewall2 (San Jose), you can configure similar rules for that device.

- The manual identity NAT rule would be for 'sanjose-network' when the destination is boulder-network. Create new interface objects for the Firewall2 inside and outside networks.
- The manual dynamic interface PAT rule would be for 'sanjose-network' when the destination is "any."

About Global IKE Policies

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

The following procedure explains how to configure the global policy through the Objects page. You can also enable, disable, and create policies when editing a VPN connection by clicking Edit for the IKE Policy settings.

The following topics explain how to configure IKE policies for each version:

- Managing IKEv1 Policies
- Managing IKEv2 Policies

Managing IKEv1 Policies

About IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv1 Policy, on page 437

Create an IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv1 Policy** to create a new IKEv1 policy.
- In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv1 properties.

- **Priority** - The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **Encryption** - The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group** - The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Lifetime** - The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).
- **Authentication** - The method of authentication to use between the two peers. For more information, see Deciding Which Authentication Method to Use.
  - **Preshared Key** - Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate** - Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer. The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.
- **Hash** - The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.

Step 5 Click **Add**.

Managing IKEv2 Policies

About IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv2 Policy, on page 439

Create an IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv2 Policy** to create a new IKEv2 policy.
- In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv2 properties.

- **Priority** - The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **State** - Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption** - The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.

- **Diffie-Hellman Group** - The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Integrity Hash** - The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Deciding Which Hash Algorithms to Use.
- **Pseudo-Random Function (PRF) Hash** - The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use.
- **Lifetime** - The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

Step 5 Click **Add**.

About IPsec Proposals

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.
- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

The following topics explain how to configure IPsec proposals for each IKE version:

- Managing an IKEv1 IPsec Proposal Object
- Managing an IKEv2 IPsec Proposal Object

Managing an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Security Cloud Control supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

Related Topics

Create an IKEv1 IPsec Proposal Object, on page 441

Create an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently,Security Cloud Control supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv1 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Select the Mode in which the IKEv1 IPsec Proposal object operates.

- **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Step 5 Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For more information, see Deciding Which Encryption Algorithm to Use.

Step 6 Select the **ESP Hash** or integrity algorithm to use for authentication. For more information, see Deciding Which Hash Algorithms to Use.

Step 7 Click **Add**.

Managing an IKEv2 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

Related Topics

Create or Edit an IKEv2 IPsec Proposal Object, on page 442

Create or Edit an IKEv2 IPsec Proposal Object

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button and select **FDM** > **IKEv2 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Configure the IKE2 IPsec proposal objects:

- **Encryption** - The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Integrity Hash** - The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use.

Step 5 Click **Add**.

Monitor FDM-Managed Device Site-to-Site Virtual Private Networks

Security Cloud Control allows you to monitor, modify, and delete existing or newly created site-to-site VPN configurations on onboarded FDM-managed devices.

Check Site-to-Site VPN Tunnel Connectivity

Use the **Check Connectivity** button to trigger a real-time connectivity check against the tunnel to identify whether the tunnel is currently Search and Filter Site-to-Site VPN Tunnels. Unless you click the on-demand connectivity check button, a check across all tunnels, available across all onboarded devices, occurs once an hour.

Note

- Security Cloud Control runs this connectivity check command on the FTD to determine if a tunnel is active or idle:

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- Model ASA device(s) tunnels will always show as **Idle**.

To check tunnel connectivity from the VPN page:

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

Step 2 Search and Filter Site-to-Site VPN Tunnels the list of tunnels for your site-to-site VPN tunnel and select it.

Step 3 In the Actions pane at the right, click **Check Connectivity**.

Site-To-Site VPN Dashboard

Security Cloud Control provides a consolidated information about site-to-site VPN connections created in the tenant.

In the left pane, click **Secure Connections** > **Site to Site VPN**. The **Site-to-Site VPN** provides the information in the following widgets:

- **Sessions & Insights**: Displays a bar graph representing Active VPN Tunnels and Idle VPN Tunnels, each in appropriate colors.
- **Issues**: Shows the total number of tunnels detected with issues.
- **Pending Deploy**: Shows the total number of tunnels with pending deployment.

By clicking on a value in the pie chart or any link in the widget, the site-to-site VPN listing page is displayed with a filter based on the selected value. For instance, in the **VPN Tunnel Status** widget, on clicking the **Active VPN Tunnels**, you will be directed to the site-to-site VPN listing page with the **Active** status filter applied, showing only the active tunnels.

Identify VPN Issues

Security Cloud Control can identify VPN issues on FTD. (This feature is not yet available for AWS VPC site-to-site VPN tunnels.) This article describes:

- Find VPN Tunnels with Missing Peers
- Find VPN Peers with Encryption Key Issues
- Find Incomplete or Misconfigured Access Lists Defined for a Tunnel
- Find Issues in Tunnel Configuration

Resolve Tunnel Configuration Issues, on page 446

Find VPN Tunnels with Missing Peers

The "Missing IP Peer" condition is more likely to occur on ASA devices than FDM-managed devices.

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Check **Detected Issues**.

Step 5 Select each device reporting an issue and look in the Peers pane at the right. One peer name will be listed. Security Cloud Control reports the other peer name as, "[Missing peer IP.]"

Find VPN Peers with Encryption Key Issues

Use this approach to locate VPN Peers with encryption key issues such as:

- IKEv1 or IKEv2 keys are invalid, missing, or mismatched
- Obsolete or low encryption tunnels

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Select each device reporting an issue and look in the Peers pane at the right. The peer information will show you both peers.

Step 5 Click on **View Peers** for one of the devices.

Step 6 Double-click the device reporting the issue in the Diagram View.

Step 7 Click **Key Exchange** in the Tunnel Details panel at the bottom. You will be able to view both devices and diagnose the key issue from that point.

Find Incomplete or Misconfigured Access Lists Defined for a Tunnel

The "incomplete or misconfigured access-list" condition could only occur on ASA devices.

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Select each device reporting an issue and look in the Peers pane at the right. The peer information shows you both peers.

Step 5 Click on **View Peers** for one of the devices.

Step 6 Double-click the device reporting the issue in the Diagram View.

Step 7 Click **Tunnel Details** in the Tunnel Details panel at the bottom. You will see the message, "Network Policy: Incomplete"

Find Issues in Tunnel Configuration

The tunnel configuration error can occur in the following scenarios:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 In the **Tunnel Issues**, click **Detected Issues** to view the VPN configuration reporting errors. You can view the configuration reporting issues .

Step 5 Select the VPN configuration reporting issues.

Step 6 In the **Peers** pane on the right, the icon appears for the peer having the issue. Hover over the icon to see the issue and resolution.

Next Step: Resolve Tunnel Configuration Issues.

Resolve Tunnel Configuration Issues

This procedure attempts to resolve these tunnel configuration issues:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn’t match the other VPN tunnel, the "IKE value Mismatch" message appears.

See Find Issues in Tunnel Configuration for more information.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the device associated with the VPN configuration reporting an issue.

Step 4 Resolve the Conflict Detected Status.

Step 5 In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 6 Select the VPN configuration reporting this issue.

Step 7 In the **Actions** pane, click the **Edit** icon.

Step 8 Click **Next** in each step until you click the **Finish** button in step 4.

Step 9 Preview and Deploy Configuration Changes for All Devices, on page 568.

Search and Filter Site-to-Site VPN Tunnels

Use the filter sidebar in combination with the search field to focus your search of VPN tunnels presented in the VPN tunnel diagram.

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Click the filter icon to open the filter pane.

Step 3 Use these filters to refine your search:

- **Filter by Device**-Click **Filter by Device**, select the device type tab, and check the devices you want to find by filtering.
- **Tunnel Issues**-Whether or not we have detected either side of the tunnel has issues. Some examples of a device having issues may be but not limited to is: missing associated interface or peer IP address or access list, IKEv1 proposal mismatches, etc. (Detecting tunnel issues is not yet available for AWS VPC VPN tunnels.)
- **Devices/Services**-Filter by type of device.
- **Status**–Tunnel status can be active or idle.
  - **Active**-There is an open session where network packets are traversing the VPN tunnel or a successful session was established and hasn't been timed-out yet. Active can assist to indicate that tunnel is active and relevant.
  - **Idle** - Security Cloud Control is unable to discover an open session for this tunnel. The tunnel may either be not in use or there is an issue with this tunnel.
- **Onboarded** - Devices could be managed by Security Cloud Control or not managed (unmanaged) by Security Cloud Control.
  - **Managed** – Filter by devices that Security Cloud Control manages.
  - **Unmanaged** – Filter by devices that Security Cloud Control does not manage.
- **Device Types** - Whether or not either side of the tunnel is a live (connected device) or model device.

Step 4 You can also search the filtered results by device name or IP address by entering that information in the search bar. The search is case-insensitive.

Onboard an Unmanaged Site-to-Site VPN Peer

Security Cloud Control will discover a site-to-site VPN tunnel when one of the peers is onboarded. If the second peer is not managed by Security Cloud Control, you can filter the list of VPN tunnels to find the unmanaged device and onboard it:

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the filter panel by clicking .

Step 4 Check **Unmanaged**.

Step 5 Select a tunnel from the table from the results.

Step 6 In the **Peers** pane on the right, click **Onboard Device** and follow the instructions on the screen.

Related Information:

- Onboard Devices and Services, on page 159
- Onboard a Threat Defense Device, on page 159

View IKE Object Details of Site-To-Site VPN Tunnels

You can view the details of the IKE objects configured on the peers/devices of the selected tunnel. These details appear in a tree structure in a hierarchy based on the priority of the IKE policy object.

Note Extranet devices don't show the IKE Objects details.

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 In the **VPN Tunnels** page, click the name of the VPN tunnel that connects the peers.

Step 3 Under **Relationships** on the right, expand the object that you want to see its details.

View Last Successful Site-to-Site VPN Tunnel Establishment Date

Procedure

Step 1 View Site-to-Site VPN Tunnel Information.

Step 2 Click the **Tunnel Details** pane.

Step 3 View the **Last Seen Active** field.

View Site-to-Site VPN Tunnel Information

The site-to-site VPN table view is a complete listing of all site-to-site VPN tunnels available across all devices onboarded to Security Cloud Control. A tunnel only exists once in this list. Clicking on a tunnel listed in the table provides an option in the right side bar to navigate directly to a tunnel's peers for further investigation.

In cases where Security Cloud Control does not manage both sides of a tunnel, you can click Onboard an Unmanaged Site-to-Site VPN Peer to open the main onboarding page an onboard the unmanaged peer. In cases where Security Cloud Control manages both side of a tunnel, the Peer 2 column contains the name of the managed device. However, in the case of an AWS VPC, the Peer 2 column contains the IP address of the VPN gateway.

To view site-to-site VPN connections in the table view:

Procedure

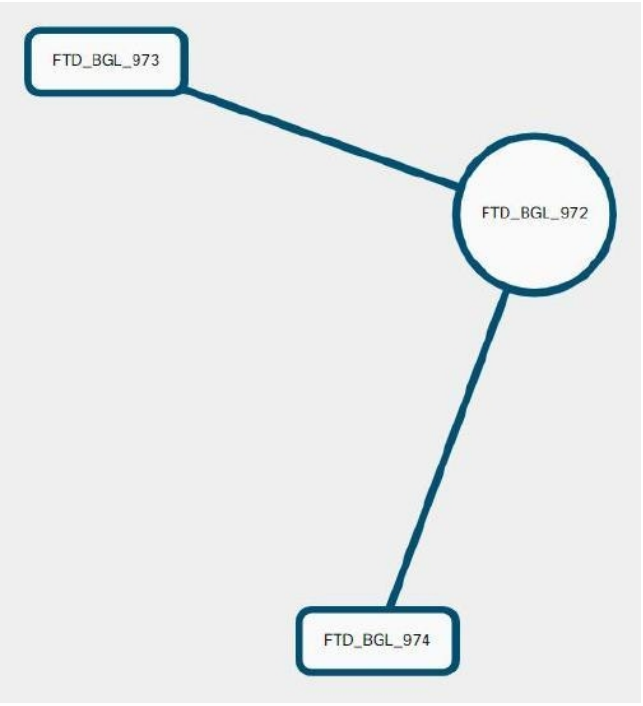
Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Click the **Table view** button.

Step 3 Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

Site-to-Site VPN Global View

This is an example fo the global view. In the illustration, 'FTD_BGL_972' has a site-to-site connection with FTD_BGL_973 and FTD_BGL_974 devices.



Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

Step 2 Click the **Global view** button.

Step 3 Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

Step 4 Select one of the peers represented in the Global View.

Step 5 Click **View Details**.

Step 6 Click the other end of the VPN tunnel and Security Cloud Control displays Tunnel Details, NAT Information, and Key Exchange information for that connection:

- **Tunnel Details**-Displays the name and connectivity information about the tunnel. Clicking the Refresh icon updates the connectivity information for the tunnels.
- **Tunnel Details specific to AWS connections**-Tunnel details for AWS site-to-site connections are slightly different than for other connections. For each connection from the AWS VPC to your VPN gateway, AWS creates two VPN tunnels. This is for high availability.
  - The name of the tunnel represents the name of the VPC your VPN gateway is connected to. The IP address named in the tunnel is the IP address that your VPN gateway knows as the VPC.
  - If the Security Cloud Control Connectivity status shows **active**, the AWS tunnel state is **Up**. If the Security Cloud Control Connectivity state is **inactive**, the AWS tunnel state is **Down**.
- **NAT Information**-Displays the type of NAT rule being used, original and translated packet information, and provides links to the NAT table to view the NAT rule for that tunnel. (Not yet available for AWS VPC site-to-site VPN.)
- **Key Exchange**-Displays the cryptographic keys in use by the tunnel and key-exchange issues. (Not yet available for AWS VPC site-to-site VPN.)

Site-to-Site VPN Tunnels Pane

The Tunnels pane displays a list of all the tunnels associated with a particular VPN gateway. For site-to-site VPN connections between your VPN gateway and an AWS VPC, the tunnels pane shows all the tunnels from your VPN gateway to the VPC. Since each site-to-site VPN connection between your VPN gateway and an AWS VPC has two tunnels, you will see double the number of tunnels you normally would for other devices.

VPN Gateway Details

Displays the number of peers connected to the VPN gateway and the IP address of the VPN gateway. This is only visible in the VPN Tunnels page.

View Peer

After you select a site-to-site VPN peer pair, the peers pane lists the two devices in the pair and allows you to click **View Peer** for one of the devices. By clicking **View Peer**, you see any other site-to-site peer that device is associated with. This is visible in the Table view and in the Global view.

Delete a Security Cloud Control Site-To-Site VPN Tunnel

Procedure

Step 1 In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

Step 2 Select the desired site-to-site VPN tunnel that you want to delete.

Step 3 In the **Actions** pane on the right, click **Delete**.

The selected site-to-site VPN tunnel is deleted.

Introduction to Remote Access Virtual Private Network

Remote Access virtual Private Network (RA VPN) capability enables users to connect to your network from a location outside the physical office premises. This means that they can use a computer or a supported iOS/Android device that is connected to the internet and access your network resources securely. This feature is particularly useful for mobile workers who need to connect from their home network or a public Wi-Fi network while ensuring that their data remains safe and protected.

Related Information:

-
- Configuring Remote Access VPN for an FDM-Managed Device

Introduction to Remote Access Virtual Private Network

Remote Access virtual Private Network (RA VPN) capability enables users to connect to your network from a location outside the physical office premises. This means that they can use a computer or a supported iOS/Android device that is connected to the internet and access your network resources securely. This feature is particularly useful for mobile workers who need to connect from their home network or a public Wi-Fi network while ensuring that their data remains safe and protected.

Related Information:

-
- Configuring Remote Access VPN for an FDM-Managed Device

Configuring Remote Access VPN for an FDM-Managed Device

Security Cloud Control provides an intuitive user interface for configuring a new Remote Access Virtual Private Network (RA VPN). It also allows you to quickly and easily configure RA VPN connection for multiple FDM-managed devices that are on board in Security Cloud Control. AnyConnect is the only client that is supported on endpoint devices for an RA VPN connectivity to FDM-managed devices.

When the AnyConnect client negotiates an SSL VPN connection with the FDM-managed device, it connects using Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. The client and the FDM-managed device negotiate the TLS/DTLS version to use. DTLS is used if the client supports it.

Security Cloud Control supports the following aspects of RA VPN functionality on FDM-managed devices:

- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple FDM-managed devices

Important If an onboarded FDM-managed device (running on software version 6.7 or later) contains RA VPN configuration with SAML server as the authentication source, Security Cloud Control doesn't populate the AAA details in the connection profile as it doesn't manage SAML server objects in the current release. Thus you can't manage such RA VPN configuration from Security Cloud Control. However, Security Cloud Control reads the RA VPN connection profile and associated trusted CA certificate and SAML server objects.

Related Information:

- Control User Permissions and Attributes Using RADIUS and Group Policies, on page 453
- End-to-End Remote Access VPN Configuration Process for an FDM-Managed Device, on page 466
  - Download AnyConnect Client Software Packages, on page 468
  - Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0, on page 468
  - Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later, on page 471
  - Upload RA VPN AnyConnect Client Profile, on page 499
  - Configure Identity Sources for FDM-Managed Device, on page 474
    - Create or Edit an Active Directory Realm Object, on page 477
    - Create or Edit a RADIUS Server Object or Group, on page 479
  - Create New RA VPN Group Policies, on page 482
  - Create an RA VPN Configuration, on page 488
  - Configure an RA VPN Connection Profile, on page 492
  - Allow Traffic Through the Remote Access VPN, on page 496
  - Upgrade AnyConnect Package on an FDM-Managed Device Running Version 6.4.0, on page 497
- Guidelines and Limitations of Remote Access VPN for FDM-Managed Device, on page 500
- How Users Can Install the AnyConnect Client Software on FDM-Managed Device, on page 501
- Licensing Requirements for Remote Access VPN, on page 504
- Maximum Concurrent VPN Sessions By Device Model, on page 504
- RADIUS Change of Authorization, on page 505
  - Configure Change of Authorization on the FDM-Managed Device, on page 505

Split Tunneling for RA VPN Users (Hair Pinning)

This article describes the split tunneling for RA VPN.

Typically, in remote access VPN, you might want the VPN users to access the Internet through your device. However, you can allow your VPN users to access an outside network while they are connected to an RA VPN. This technique is called split tunneling or hair pinning. The split tunnel allows VPN connectivity to a remote network across a secure tunnel, and it also allows connectivity to a network outside the VPN tunnel. Split tunneling reduces the network load on the FDM-managed devices and increases the bandwidth on the outside interface.

To configure a split-tunnel list, you must create a Standard Access List or Extended Access List. Follow the instructions explained in the **How to Provide Internet Access on the Outside Interface for Remote Access VPN Users (Hair Pinning)** section of Virtual Private Networks (VPN) chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Control User Permissions and Attributes Using RADIUS and Group Policies

This article provides information on applying attributes to RA VPN connections from an external RADIUS server or a group policy.

You can apply user authorization attributes (also called user entitlements or permissions) to RA VPN connections from an external RADIUS server or from a group policy defined on the FDM-managed device. If the FDM-managed device receives attributes from the external AAA server that conflict with those configured on the group policy, then attributes from the AAA server always take precedence.

The FDM-managed device applies attributes in the following order:

Procedure

Step 1 User attributes defined on the external AAA server - The server returns these attributes after successful user authentication or authorization.

Step 2 Group policy configured on the FDM-managed device - If a RADIUS server returns the value of the RADIUS CLASS attribute IETF-Class-25 (OU= group-policy) for the user, the FDM-managed device places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.

Step 3 Group policy assigned by the connection profile - The connection profile has the preliminary settings for the connection and includes a default group policy applied to the user before authentication. All users connecting to the FDM-managed device initially belong to this group, which provides any attributes that are missing from the user attributes returned by the AAA server, or the group policy assigned to the user.

FDM-managed devices support RADIUS attributes with vendor ID 3076. If the RADIUS server you use does not have these attributes defined, you must manually define them. To define an attribute, use the attribute name or number, type, value, and vendor code (3076).

The following topics explain the supported attributes based on whether the values are defined in the RADIUS server, or whether they are values the system sends to the RADIUS server.

Attributes Sent to the RADIUS Server

RADIUS attributes 146 and 150 are sent from the FDM-managed device to the RADIUS server for authentication and authorization requests. All the following attributes are sent from the FDM-managed device to the RADIUS server for accounting start, interim-update, and stop requests.

Table 16: Attributes Secure Firewall Threat Defense Sends to RADIUS

Attribute	Attribute	Syntax, Type	Single or Multi-valued	Description or Value
Client Type	150	Integer	Single	The type of client this is connecting to the VPN: 2= AnyConnect Client SSL VPN
Session Type	151	Integer	Single	The type of connection: 1 = AnyConnect Client SSL VPN
Tunnel Group Name	146	String	Single	The name of the connection profile that was used for establishing the session, as defined on the FDM-managed device. The name can be 1 - 253 characters.

Attributes Received from the RADIUS Server

The following user authorization attributes are sent to the FDM-managed device from the RADIUS server.

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Access-List-Inbound	86	String	Single	Both Access-List attributes take the name of an ACL that is configured on the FDM-managed device. Create these ACLs in firewall device manager using the Smart CLI Extended Access List object type (Log in to firewall device manager and select **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**). These ACLs control traffic flow in the inbound (traffic entering the FDM-managed device) or outbound (traffic leaving the FDM-managed device) direction.
Access-List-Outbound	87	String	Single	
Address-Pools	217	String	Single	The name of a network object defined on the FDM-managed device that identifies a subnet, which will be used as the address pool for clients connecting to the RA VPN. Define the network object on the **Objects** page.
Banner1	15	String	Single	The banner to display when the user logs in.
Banner2	36	String	Single	The second part of the banner to display when the user logs in. Banner2 is appended to Banner1.

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Group-Policy	25	String	Single	The group policy to use in the connection. You must create the group policy on the RA VPN **Group Policy** page. You can use one of the following formats: • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	Integer	Single	The number of separate simultaneous connections the user can establish, 0 - 2147483647.
VLAN	140	Integer	Single	The VLAN on which to confine the user's connection, 0 - 4094. You must also configure this VLAN on a subinterface on the FDM-managed device.

Two-Factor Authentication

You can configure two-factor authentication for the RA VPN. With two-factor authentication, the user must supply a username and static password, plus an additional item such as a Duo passcode. Two-factor authentication differs from using a second authentication source in that two-factor is configured on a single authentication source, with the relationship to the Duo server tied to the primary authentication source. The exception is Duo LDAP, where you configure the Duo LDAP server as the secondary authentication source.

- Duo Two-Factor Authentication Using RADIUS, on page 456
- Duo Two-Factor Authentication using LDAP, on page 461

Duo Two-Factor Authentication Using RADIUS

You can configure the Duo RADIUS server as the primary authentication source. This approach uses the Duo RADIUS Authentication Proxy.

For the detailed steps to configure Duo, please see https://duo.com/docs/cisco-firepower.

You would then configure Duo to forward authentication requests directed to the proxy server to use another RADIUS server, or a Microsoft Active Directory(AD) server, as the first authentication factor, and the Duo Cloud Service as the second factor.

When using this approach, the user must authenticate using a username that is configured on both the Duo Authentication Proxy and the associated RADIUS/AD server, and the password for the username configured in the RADIUS/AD server, followed by one of the following Duo codes:

Duo-passcode. For example, my-password,12345.

push. For example, *my-password*,**push**. Use **push** to tell Duo to send a push authentication to the Duo Mobile app, which the user must have already installed and registered.

sms. For example, *my-password*,**sms**. Use sms to tell Duo to send an SMS message with a new batch of passcodes to the user's mobile device. The user's authentication attempt will fail when using sms. The user must then re-authenticate and enter the new passcode as the secondary factor.

phone. For example, *my-password*,**phone**. Use phone to tell Duo to perform phone callback authentication.

If the username and password are authenticated, the Duo Authentication Proxy contacts the Duo Cloud Service, which validates that the request is from a valid configured proxy device and then pushes a temporary passcode to the mobile device of the user as directed. When the user accepts this passcode, the session is marked authenticated by Duo and the RA VPN is established.

For a detailed explanation, see How to Configure Two-Factor Authentication using Duo RADIUS, on page 457

How to Configure Two-Factor Authentication using Duo RADIUS

You can configure the Duo RADIUS server as the primary authentication source. This approach uses the Duo RADIUS Authentication Proxy.

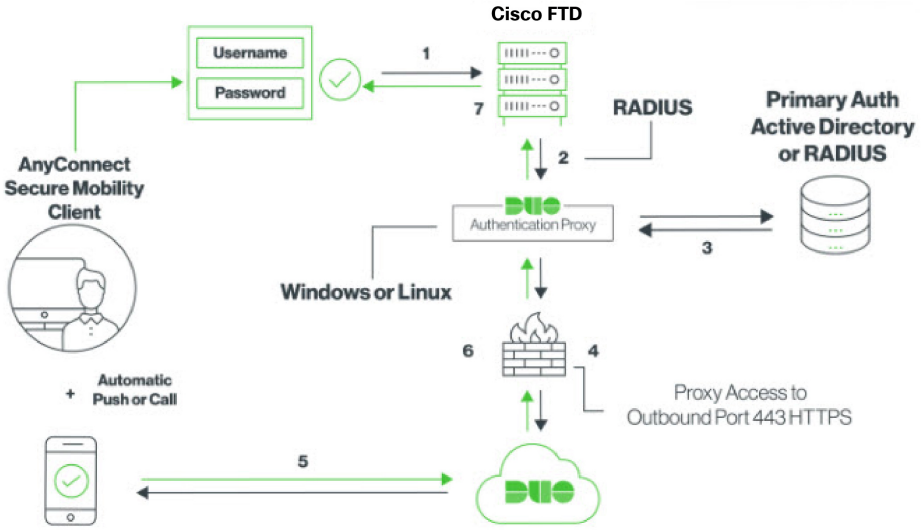
You would then configure Duo to forward authentication requests directed to the proxy server to use another RADIUS server, or an AD server, as the first authentication factor, and the Duo Cloud Service as the second factor.

The following topics explain the configuration in more detail:

- System Flow for Duo RADIUS Secondary Authentication, on page 457
- Configure Device for Duo RADIUS Using Security Cloud Control, on page 459

System Flow for Duo RADIUS Secondary Authentication

Following is an explanation of the system



flow:

1. The user makes a remote access VPN connection to the FDM-managed device and provides username associated with RADIUS/AD server, the password for the username configured in the RADIUS/AD server, followed by one of the DUO codes, Duo-password, push, SMS, or phone. For more information, Duo Two-Factor Authentication Using RADIUS, on page 456
2. FDM-managed device sends the authentication request to the Duo Authentication proxy.
3. Duo Authentication proxy authenticates this primary authentication attempt with the primary authentication server, which might be Active Directory or RADIUS.
4. If the credentials are authenticated, the Duo Authentication Proxy connection is established to Duo Security over TCP port 443.
5. Duo then authenticates the user separately through push notification, text message with a passcode, or a telephone call. The user must complete this authentication successfully.
6. Duo authentication proxy receives the authentication response.
7. If the secondary authentication was successful, the FDM-managed device establishes a remote access VPN connection with the user's AnyConnect client.

Configure Duo RADIUS Secondary Authentication

Duo Authentication proxy authenticates this primary authentication attempt with the primary authentication server, which might be Active Directory or RADIUS.

Create a Duo Account

Create a Duo account and obtain the integration key, secret key, and API hostname.

Following is an overview of the process. For details, please see the Duo web site,

Procedure

Step 1 Sign up for a Duo account.

Step 2 Log in to the Duo Admin Panel and navigate to **Applications**.

Step 3 Click **Protect an Application** and locate **Cisco Firepower Threat Defense VPN** in the applications list.

Step 4 Click **Protect this Application** to get your integration key, secret key, and API hostname. You'll need this information when configuring the proxy. For help, see the *Duo Getting Started* guide, https://duo.com/docs/getting-started.

Step 5 Install and configure the Duo Authentication Proxy. For instructions, see the "Install the Duo Authentication Proxy" section in https://duo.com/docs/cisco-firepower.

Step 6 Start the Authentication Proxy. For instructions, see the "Start the Proxy" section in https://duo.com/docs/cisco-firepower.

For enrolling new users in Duo, see https://duo.com/docs/enrolling-users.

Configure Device for Duo RADIUS Using Security Cloud Control

Procedure

Step 1 Configure FTD Radius Server Object.

a) In the left pane, click **Objects > FDM Objects**.

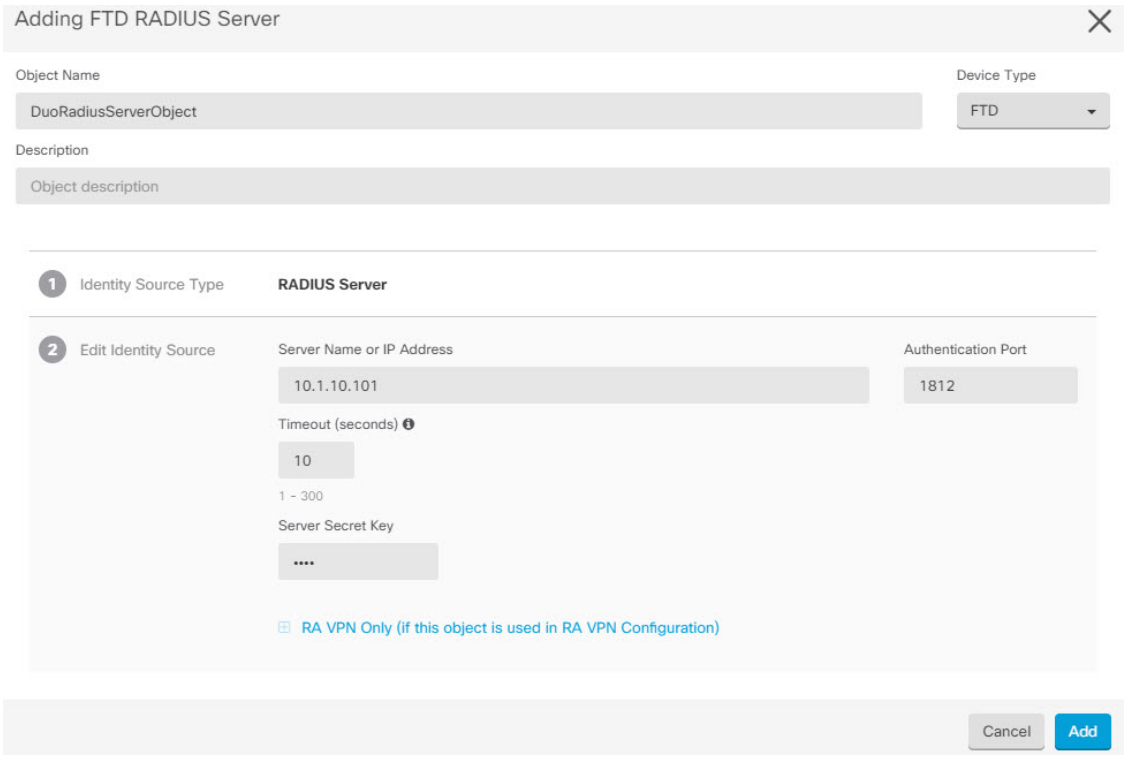
b) Click  > **RA VPN Objects (ASA & FTD)** > **Identity Source**.

c) Provide a name and set the **Device Type** as **FTD**.

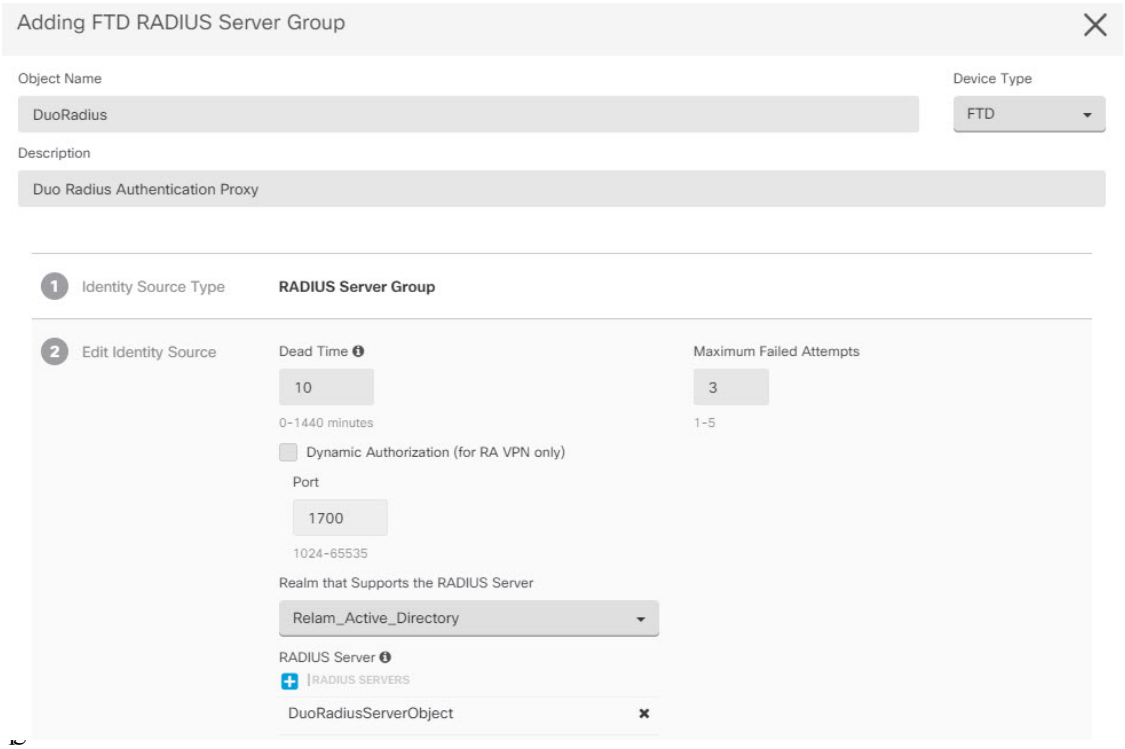
d) Select **Radius Server Group** and click **Continue**. For details, see step 6 in Create a RADIUS Server Group, on page 480.

e) In the **Radius Server** section, click the **Add** button and click **Create New Radius Server**. See Create a RADIUS Server Object, on page 479

In the **Server Name or IP Address** field, enter your Duo Authentication Proxy server's fully-qualified hostname or IP address.

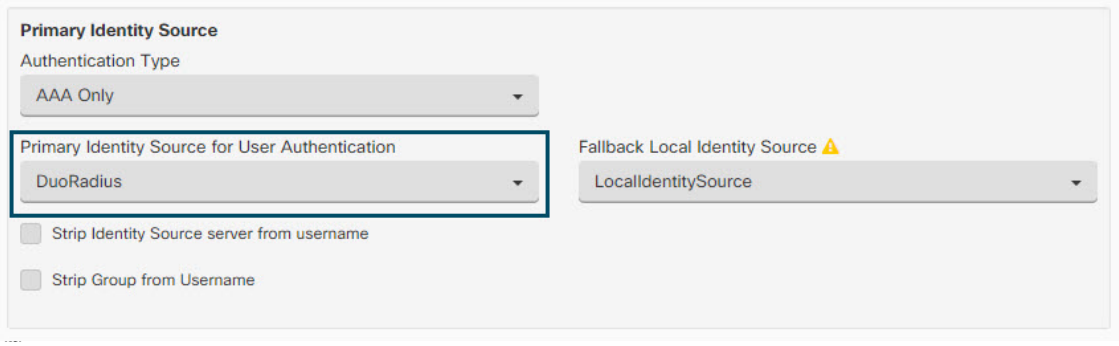


f) Once you have added the Duo RADIUS server to the group, click **Add** to create the new Duo RADIUS server



Step 2 Change the Remote Access VPN Authentication Method to Duo RADIUS.

a) In the left pane, click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**.
b) Expand the VPN configuration and click on the connection profile to which you want to add Duo.
c) In the **Actions** pane on the right, click **Edit**.
d) Select the **Authentication Type** can be **AAA** or **AAA and Client Certificate**.
e) In the **Primary Identity Source for User Authentication** list, select the server group you created



f) You typically do not need to select an "Authorization Server" or "Accounting Server".
g) Click **Continue**.
h) In the **Summary and Instructions** step, click **Done** to save the configuration.

Step 3 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Duo Two-Factor Authentication using LDAP

You can use the Duo LDAP server as the secondary authentication source along with a Microsoft Active Directory (AD) or RADIUS server as the primary source. With Duo LDAP, the secondary authentication validates the primary authentication with a Duo passcode, push notification, or phone call.

Note The Duo two-factor authentication feature is available in Security Cloud Control for devices running Firepower Threat Upgrade a Single FDM-Managed Device.

The FDM-managed device communicates with Duo LDAP using LDAPS over port TCP/636.

When using this approach, the user must authenticate using a username that is configured on both the AD/RADIUS server and the Duo LDAP server. When prompted to log in by AnyConnect, the user provides the AD/RADIUS password in the primary Password field, and for the Secondary Password, provides one of the following to authenticate with Duo. For more details, see the "Second Password for Factor Selection" section in https://guide.duo.com/anyconnect.

- *Duo passcode*—Authenticate using a passcode, either generated with Duo Mobile, sent via SMS, generated by your hardware token, or provided by an administrator. For example, 1234567.
- **push**—Push a login request to your phone, if you have installed and activated the Duo Mobile app. Review the request and tap **Approve** to log in.
- **phone**—Authenticate using a phone callback.
- **sms**—Request a Duo passcode in a text message. The login attempt will fail. Log in again using the new passcode.

For a detailed explanation, see How to Configure Two-Factor Authentication using Duo LDAP, on page 462.

How to Configure Two-Factor Authentication using Duo LDAP

You can use the Duo LDAP server as the secondary authentication source along with a Microsoft Active Directory (AD) or RADIUS server as the primary source. With Duo LDAP, the secondary authentication validates the primary authentication with a Duo passcode, push notification, or phone call..

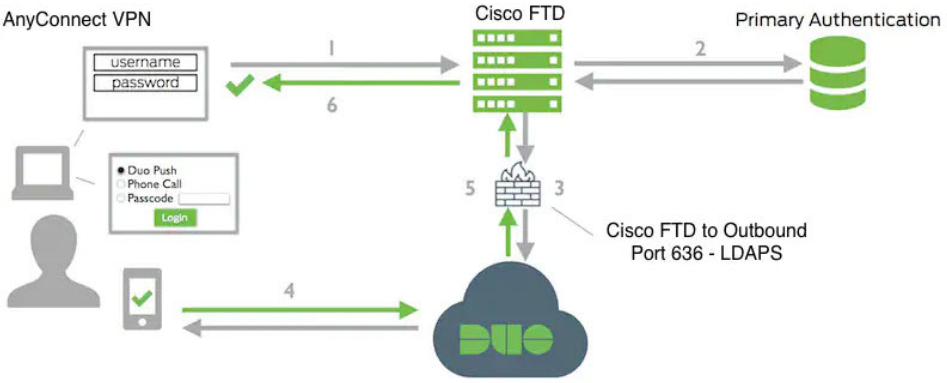
The following topics explain the configuration in more detail:

- System Flow for Duo LDAP Secondary Authentication, on page 462
- Configure Duo LDAP Secondary Authentication, on page 462

System Flow for Duo LDAP Secondary Authentication

The following graphic shows how threat defense and Duo work together to provide two-factor authentication using LDAP.

Following is an explanation of the system flow:



1. The user makes a remote access VPN connection to the FDM-managed device and provides username and password.
2. FDM-managed device authenticates this primary authentication attempt with the primary authentication server, which might be Active Directory or RADIUS.
3. If the primary authentication works, FDM-managed device sends a request for secondary authentication to the Duo LDAP server.
4. Duo then authenticates the user separately, through push notification, text message with a passcode, or a telephone call. The user must complete this authentication successfully.
5. Duo responds to the FDM-managed device to indicate whether the user authenticated successfully.
6. If the secondary authentication was successful, the FDM-managed device establishes a remote access VPN connection with the user's AnyConnect client.

Configure Duo LDAP Secondary Authentication

The following procedure explains the end-to-end process of configuring two-factor authentication, using Duo LDAP as the secondary authentication source, for remote access VPN. You must have an account with Duo, and obtain some information from Duo, to complete this configuration.

Create a Duo Account

Create a Duo account and obtain the integration key, secret key, and API hostname.

Following is an overview of the process. For details, please see the Duo web site,

Procedure

Step 1 Sign up for a Duo account.

Step 2 Log in to the Duo Admin Panel and navigate to **Applications**.

Step 3 Click **Protect an Application** and locate **Cisco Firepower Threat Defense VPN** in the applications list.

Step 4 Click **Protect this Application** to get your **Integration key**, **Secret key**, and **API hostname**. For help, see the *Duo Getting Started* guide, https://duo.com/docs/getting-started.

For enrolling new users in Duo, see https://duo.com/docs/enrolling-users.

Upload a Trusted CA Certificate to an FDM-Managed Device

The FDM-managed device must have the trusted CA certificate needed to validate the connection to the Duo LDAP server. You can go directly to https://www.digicert.com/digicert-root-certificates.htm and download either **DigiCertSHA2HighAssuranceServerCA** or **DigiCert High Assurance EV Root CA** and upload it using Firewall Device Manager (FDM).

Procedure

Step 1 Access the firewall device manager page of the FDM-managed device, choose **Objects** > **Certificates**.

Step 2 Click **+** > **Add Trusted CA Certificate**.

Step 3 Enter a name for the certificate, for example, DigiCert_High_Assurance_EV_Root_CA. (Spaces are not allowed.)

Step 4 Click **Upload Certificate** and select the file that you downloaded.

Step 5 Click **OK**.

Step 6 Onboard the device to Security Cloud Control if you haven't onboarded it already.

Step 7 Read All Device Configurations.

Configure FTD for Duo LDAP in Security Cloud Control

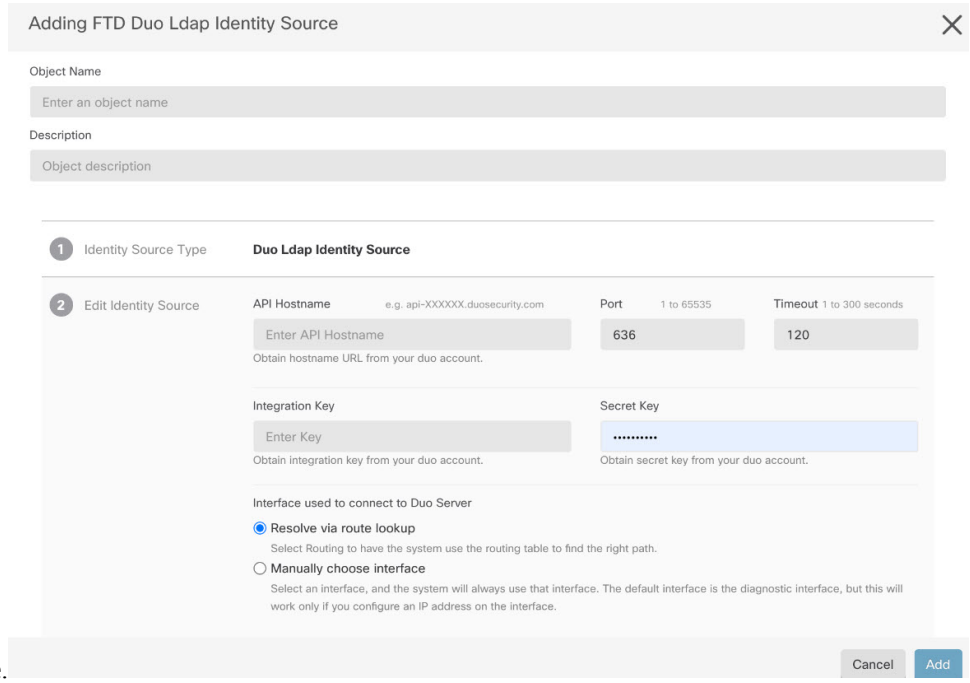
Procedure

Step 1 Create a Duo LDAP identity source object for the Duo LDAP server.

a) In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

b) Click the  to create an object > **RA VPN Objects (ASA & FTD)** > **Identity Source**.

c) Enter a name for the object, for example, Duo-LDAP-server.
d) Select the **Device Type** as **FTD**.
e) Click **Duo Ldap Identity Source** and click



Continue.

f) In the **Edit Identity Source** area, provide the following details:

- **API Hostname**: Enter the API Hostname that you obtained from your Duo account. The hostname should look like the following, with the X's replaced with your unique value: API-XXXXXXXX.DUOSECURITY.COM. Uppercase is not required.
- **Port**: Enter the TCP port to use for LDAPS. This should be 636 unless you have been told by Duo to use a different port. Note that you must ensure that your access control list allows traffic to the Duo LDAP server through this port.
- **Timeout**: Enter the timeout, in seconds, to connect to the Duo server. The value can be 1-300 seconds. The default is 120. To use the default, either enter 120 or delete the attribute line.
- **Integration Key**: Enter the integration key that you obtained from your Duo account.
- **Secret Key**: Enter the secret key that you obtained from your Duo account. This key will subsequently be masked.
- **Interface used to connect to Duo Server**: Select the interface that is used for connecting to Duo Server.
  - **Resolve via route lookup**: Select this option to use the routing table to find the right path. For creating a routing table, see Routing.
  - **Manually choose interface**: Select this option and choose one of the interfaces from the list. The default interface is the diagnostic interface, but this will work only if you configure an IP address on the interface. Note: Ensure that the selected interface is present on the same device you want to connect to Duo Server.
  - Click **Add**.

Step 2 (optional) Use the AnyConnect Profile Editor to create a profile that specifies 60 seconds or more for authentication timeout.

You need to give users extra time to obtain the Duo passcode and complete the secondary authentication. We recommend at least 60 seconds. The following procedure explains how to configure the authentication timeout only and then upload the profile to FDM-managed device. If you want to change other settings, you can do so now.

a) If you have not already done so, download and install the AnyConnect profile editor package. You can find this in the Cisco Software center (software.cisco.com) in the folder for your AnyConnect version. The base path at the time of this writing is **Downloads Home** > **Security** > **VPN and Endpoint Security Clients** > **Cisco VPN Clients** > **AnyConnect Secure Mobility Client**.
b) Open the AnyConnect **VPN Profile Editor**.
c) Select **Preferences (Part 2)** in the table of contents, scroll to the end of the page, and change **Authentication Timeout** to 60 (or more). The following image is from the AnyConnect 4.7 VPN Profile Editor; previous or subsequent versions might be different.
d) Choose **File** > **Save**, and save the profile XML file to your workstation with an appropriate name, for example, duo-ldap-profile.xml.
e) You can now close the **VPN Profile Editor** application.
f) In Security Cloud Control, Upload RA VPN AnyConnect Client Profile.

Step 3 Create a group policy and select the AnyConnect profile in the policy.

The group policy that you assign to a user controls many aspects of the connection. The following procedure explains how to assign the profile XML file to the group. For more information, see Create New RA VPN Group Policies.

a) In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.
b) To edit an existing group policy, use the **RA VPN Group Policy** filter to view only the existing group policies and modify the policy that you want and save it.
c) To create a new group policy, click **RA VPN Objects (ASA & FTD)** > **RA VPN Group Policy**.
d) On the **General** page, configure the following properties:

- **Name** — For a new profile, enter a name. For example, Duo-LDAP-group.
- **AnyConnect Client Profiles** — Select the AnyConnect client profile object that you created.

e) Click **Add** to save the object.
f) Click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**.
g) Click the remote access VPN configuration that you want to update.
h) In the **Actions** pane on the right, click **Group Policies**.
i) Click **+** to select the group policies that you want to associate with the VPN configuration.
j) Click **Save** to save the group policy.

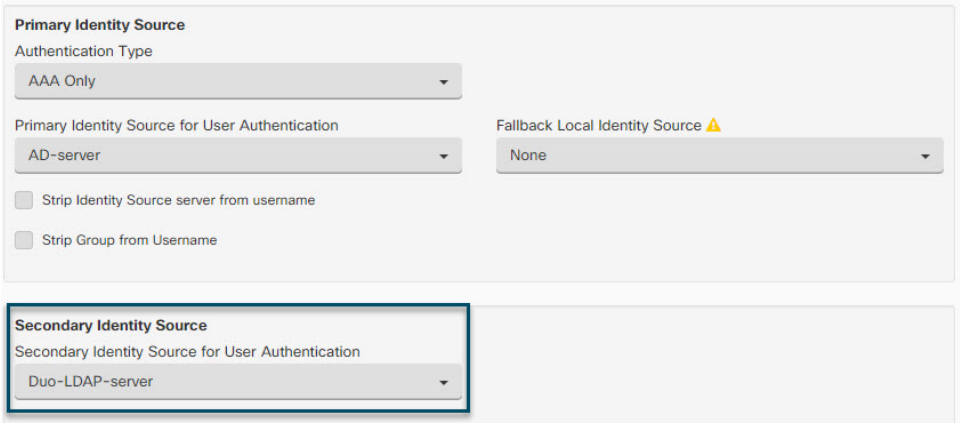
Step 4 Create or edit the remote access VPN connection profile to use for Duo-LDAP secondary authentication.

The following procedure just mentions the key changes to enable Duo-LDAP as the secondary authentication source and apply the AnyConnect client profile. For new connection profiles, you must configure the rest of the required fields. For this procedure, we assume you are editing an existing connection profile, and you simply must change these two settings.

a) On the Security Cloud Control navigation page, click **VPN** > **Remote Access VPN Configuration**.
b) Expand the remote access VPN configuration and click the connection profile that you want to update.
c) In the **Actions** pane on the right, click **Edit**.

d) Under **Primary Identity Source**, configure the following:

- **Authentication Type** — Choose either AAA Only or AAA and Client Certificate. You cannot configure two-factor authentication unless you use AAA.
- **Primary Identity Source for User Authentication** — Select your primary Active Directory or RADIUS server. Note that you can select a Duo-LDAP identity source as the primary source. However, Duo-LDAP provides authentication services only, not identity services, so if you use it as a primary authentication source, you will not see usernames associated with RA VPN connections in any dashboards, and you will not be able to write access control rules for these users. (You can configure fallback to the local identity source if you want to.)
- **Secondary Identity Source** — Select the Duo-LDAP identity source.



Note If username in **Primary Identity Source** and **Secondary Identity Source** are the same, we recommend enabling **Use Primary username for Secondary login** in the **Advanced** options in the Connection Profile. Configuring this way allows the end-user to use a single username for both primary and secondary identity sources.

e) Click **Continue**.

f) On the **Group Policy** page, select the group policy that you created or

g) Click **Continue**.

h) Click **Done** to save your changes to the connection profile.

Step 5 Preview and Deploy Configuration Changes for All Devices, on page 568.

End-to-End Remote Access VPN Configuration Process for an FDM-Managed Device

This section provides the end-to-end procedure for configuring Remote Access Virtual Private Network (RA VPN) on an FDM-managed device onboarded to Security Cloud Control.

To enable remote access VPN for your clients, you need to configure several separate items. The following procedure provides the end-to-end process.

Procedure

Step 1 Enable two licenses.

- When you register the device, you must do so with a Smart Software Manager account that is enabled for export-controlled features. The license must meet export control requirements before you can configure remote access VPN. You also cannot configure the feature using the evaluation license. Your purchase of an FDM-managed device automatically includes an license. The license covers all features not covered by the optional licenses. It is a perpetual license. The device must be registered to Secure Firewall device manager. See the **Registering the Device** section in the Licensing the System chapter of the Cisco Secure Firewall Threat Defense Configuration Guide for the version your device is running.
- A license. For details, see Licensing Requirements for Remote Access VPN.
  - To enable the license, see the **Enabling or Disabling Optional Licenses** section in the Licensing the System chapter of the Secure Firewall Threat Defense Configuration Guide for the version your device is running.

Step 2 Configure Certificates.

Certificates are required to authenticate SSL connections between the clients and the device. You can use the pre-defined DefaultInternalCertificate for the VPN or create your own.

If you use an encrypted connection for the directory realm used for authentication, you must upload a trusted CA certificate. For more information on certificates and how to upload them, see Configuring Certificates.

Step 3 Configure the identity source used for authenticating remote users.

You can use the following sources to authenticate users attempting to connect to your network using RA VPN. Additionally, you can use client certificates for authentication, either alone or in conjunction with an identity source.

- Active Directory identity realm: As a primary authentication source. The user accounts are defined in your Active Directory (AD) server. See Configuring AD Identity Realms. See Create or Edit an Active Directory Realm Object.
- RADIUS server group: As a primary or secondary authentication source, and for authorization and accounting. See Create or Edit a RADIUS Server Object or Group.
- Local Identity Source (the local user database): As a primary or fallback source. You can define users directly on the device and not use an external server. If you use the local database as a fallback source, ensure that you define the same usernames/passwords as the ones described in the external server.

  Note You can create user accounts directly on the FDM-managed device only from Secure Firewall device manager. See Configure Local Users.

Step 4 (Optional.) Create New RA VPN Group Policies.

The group policy defines user-related attributes. You can configure group policies to provide differential access to resources based on group membership. Alternatively, use the default policy for all connections.

Step 5 Create an RA VPN Configuration.

Step 6 Configure an RA VPN Connection Profile.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Step 8 Allow Traffic Through the Remote Access VPN.

Step 9 (Optional.) Enable the identity policy and configure a rule for passive authentication. If you enable passive user authentication, users who logged in through the remote access VPN will be shown in the dashboards, and they will also be available as traffic-matching criteria in policies. If you do not enable passive authentication, RA VPN users will be available only if they match an active authentication policy. You must enable the identity policy to get any username information in the dashboards or for traffic matching. See Configure Identity Policies.

Important If you change the Remote Access VPN configuration by using a local manager like Secure Firewall device manager, the **Configuration Status** of that device in Security Cloud Control shows "Conflict Detected". See Out-of-Band Changes on Devices. You can Resolve Configuration Conflicts on this FDM-managed device.

What to do next

Once the RA VPN configuration is downloaded to the FDM-managed devices, the users can connect to your network from a remote location using a computer or other supported iOS or Android device connected to the Internet. You can monitor live AnyConnect Remote Access Virtual Private Network (RA VPN) sessions from all onboarded RA VPN head-ends in your tenant. See Monitor Remote Access Virtual Private Network Sessions.

Download AnyConnect Client Software Packages

Before configuring a remote access VPN, you must download the AnyConnect software packages from https://software.cisco.com/download/home/283000185 to your workstation. Ensure that you download the "AnyConnect Headend Deployment Package" for your desired operating systems. Later, you can upload these packages to FDM-managed devices when defining the VPN.

Always download the latest AnyConnect version, to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the device.

Note You can upload one AnyConnect package per Operating System (OS): Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0

You can upload the AnyConnect software packages to the FDM-managed devices version 6.4.0 using firewall device manager API explorer. A minimum of one AnyConnect software package must be present on the device to create an RA VPN connection.

Important The procedure applies only to firewall device manager Version 6.4. If you are using firewall device manager Version 6.5 or later, use the Security Cloud Control interface to Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later.

Use the following procedure to upload the AnyConnect package to firewall device manager Version 6.4.0:

Procedure

Step 1 Download the AnyConnect packages from https://software.cisco.com/download/home/283000185.

- Make sure you accept the EULA and have K9 (encrypted image) privileges.
- Select the "AnyConnect Headend Deployment Package" package for your operating system. The package name will be similar to, "anyconnect-win-4.7.04056-webdeploy-k9.pkg. There are separate headend Webs Deploy packages for Windows, macOS, and Linux.

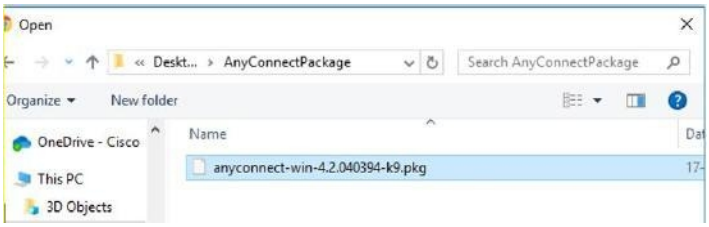
Step 2 Using a browser, open the home page of the system. For example, https://ftd.example.com.

Step 3 Log into Firewall Device Manager.

Step 4 Edit the URL to point to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

Step 5 Scroll down and click **Upload** > **/action/uploaddiskfile.**

Step 6 In **fileToUpload** field**,** click **Choose File** and select the required AnyConnect package. You can upload the packages one at a time.



Step 7 Click **Open**.

Step 8 Scroll down and click **TRY IT OUT!.** Wait until the package uploads completely. In the **Response Body**, the API response appears in the following format.

{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"type": "fileuploadstatus",

"links": {

"self":

https://ftd.example.com:972/api/fdm/...90d111e9-a361- cf32937ce0df.pkg

} }

Record the **fileName** of the package from the response as you must enter the same string when performing the POST operation. In this example, the fileName is **691f47e1-90c7-11e9-a361-79e2452f0c57.pkg**.

Step 9 Scroll up near the top of Threat Defense REST API page and click **AnyConnectPackageFile** > **POST /object/anyconnectpackagefiles**. Perform a POST operation to the API providing the temp staged diskFilename and the OS type of the package file in the payload. This action creates the AnyConnect package file.

Step 10 In the **body** field, enter the package details in the following format only:

{ "platformType": "WINDOWS",

"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"type": "anyconnectpackagefile",
"name": "AnyConnectWindowsBGL" }

a. In the **platformType** field, enter the OS platform as WINDOWS, MACOS, or LINUX.

b. In the **diskFileName** field, enter the **fileName** that you have recorded after uploading disk file.

c. In the **name** field, enter a name that you want for the package.

d. Click **TRY IT OUT!**.

In the **Response Body** field, the API response appears in the following format after a successful POST operation.

{ "version": "ni7xeneslft3p",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":
"https:/>/ftd.example.com:972...1-cf32937ce0df"
}
}

The AnyConnect package is created on firewall device manager.

Step 11 Click **AnyConnectPackageFile** > **GET /object/anyconnectpackagefiles** > **TRY IT OUT!.**

The **Response Body** shows all AnyConnect package files.

A sample response is shown below.

{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {
"self":
"https://ftd.example.com:972...1-23534f081c43"

```
}
}
],
```

Step 12 Upload other AnyConnect packages for each OS type. Repeat steps from 4 to 10.

Step 13 Edit the URL to point to the web page, for example, https://ftd.example.com

Step 14 Click the **Deploy Changes** icon in the upper right of the web page. The icon is highlighted with a dot when there are undeployed changes.

Step 15 If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately. The window will show that the deployment is in progress. You can close the window or wait for the deployment to complete.

Note To delete a package from the FDM-managed device, click **AnyConnectPackageFile** > **Delete**. In the **objID** field, type the package id and click **TRY IT OUT!**.

To complete a VPN connection, your users must install the AnyConnect client software on their workstation. For more information, see How Users Can Install the AnyConnect Client Software on FDM-Managed Device, on page 501.

Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later

If you're using an FDM-managed device, running Upgrade a Single FDM-Managed Device, for configuring RA VPN, you can use the RA VPN wizard in Security Cloud Control to upload AnyConnect software packages to the device. In the RA VPN wizard, you must provide the URL of the remote HTTP or HTTPS server where the AnyConnect packages are preloaded.

Note You can upload the AnyConnect package using the Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0 as well.

Upload an AnyConnect Package from Security Cloud Control Repository

The remote access VPN Configuration wizard presents AnyConnect packages per operating system from the Security Cloud Control repository, which you can select and upload to device. Make sure that the device has access to the internet and proper DNS configuration.

Note If the desired package is unavailable in the presented list or the device has no access to the internet, you can upload the package using the server where the AnyConnect packages are preloaded.

Procedure

Step 1 Click on the field that corresponds to an operating system and select an AnyConnect package.

Step 2 Click  to upload the package. If the checksum doesn't match, the AnyConnect package upload fails. You can see the device's workflow tab for more details about the failure.

Before you Begin

Make sure that you download the "AnyConnect Headend Deployment Package" for your desired operating systems. Always download the latest AnyConnect version, to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the device.

Note You can upload one AnyConnect package per Operating System (OS): Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Procedure

Step 1 Download the AnyConnect packages from https://software.cisco.com/download/home/283000185.

- Make sure you accept the EULA and have K9 (encrypted image) privileges.
- Select the "AnyConnect Headend Deployment Package" package for your operating system. The package name will be similar to "anyconnect-win-4.7.04056-webdeploy-k9.pkg." There are separate headend packages for Windows, macOS, and Linux.

Step 2 Upload the AnyConnect packages to a remote HTTP or HTTPS server. Ensure that there is a network route from the FDM-managed device to the HTTP or HTTPS server.

Note If you are uploading the AnyConnect package to an HTTPS server, ensure that the following steps are performed:

- Upload the trusted CA certificate of that server on the FDM-managed device from firewall device manager. To upload the certificate, see the "Uploading Trusted CA Certificates" section in the "Certificates" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version X.Y.
- Install the trusted CA certificate on the HTTPS server.

Step 3 The remote server's URL must be a direct link without prompting for authentication. If the URL is pre-authenticated, the file can be downloaded by specifying the RA VPN wizard's URL.

Step 4 If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Upload new AnyConnect Packages

Use the following procedure to upload a new AnyConnect packages to an FDM-managed device running Version 6.5.0:

Procedure

Step 1 Create an RA VPN Configuration.

Step 2 In the **AnyConnect Package Detected**, you can upload separate packages for Windows, Mac, and Linux endpoints.

Step 3 In the corresponding platform field, specify the server's paths where the AnyConnect packages compatible for Windows, Mac, and Linux are pre-uploaded. Examples of server paths: 'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

Step 4 Click to upload the package. Security Cloud Control validates if the path is reachable, and the specified filename is a valid package. When the validation is successful, the names of the AnyConnect packages appear. As you add more FDM-managed devices to the RA VPN configuration, you can upload the AnyConnect packages to them.

Step 5 Click **OK**. The AnyConnect packages are added to the RA VPN configuration.

Step 6 Continue to perform procedure in Create an RA VPN Configuration from here onwards.

What to do next

To complete a VPN connection, users must install the AnyConnect client software on their workstation. For more information, see How Users Can Install the AnyConnect Client Software on FDM-Managed Device.

Replace an Existing AnyConnect Package

If the AnyConnect packages are already present on the devices, you can see them in the RA VPN wizard. You can see all the available AnyConnect packages for an operating system in a drop-down list. You can select an existing package from the list and replace it with a new one but can't add a new package to the list.

Note If you want to replace an existing package with a new one, ensure that the new AnyConnect package is uploaded already to a server on the network that the FDM-managed device can reach.

Procedure

Step 1 In the left pane, click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**.

Step 2 Select the RA VPN configuration to be modified, and under **Actions**, click **Edit**.

Step 3 In **AnyConnect Packages Detected**, click icon appearing beside the existing AnyConnect package. If there are multiple versions of AnyConnect package for an operating system, select the package you want to replace from the list and click **Edit**. The existing package disappears from the corresponding field.

Step 4 Specify the server's path where the new AnyConnect package is preloaded and click to upload the package.

Step 5 Click **OK**. The new AnyConnect package is added to the RA VPN configuration.

Step 6 Continue to Create an RA VPN Configuration from step 6 onwards.

Delete the AnyConnect Package

Procedure

Step 1 In the left pane, click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**.

Step 2 Select the RA VPN configuration to be modified, and under **Actions**, click **Edit**.

Step 3 In **AnyConnect Packages Detected**, click icon appearing beside the AnyConnect package that you want to delete. If there are multiple versions of AnyConnect package for an operating system, select the package you want to delete from the list. The existing package disappears from the corresponding field.

Note Click **Cancel** to stop the delete operation and retain the existing package.

Step 4 Click **OK**. The device's **Configuration Status** is in 'Not Synced' state.

Note If you want to undo the delete action at this stage, go to **Inventory** page and click **Discard Changes** to retain the existing AnyConnect package.

Step 5 Preview and Deploy Configuration Changes for All Devices.

Configure Identity Sources for FDM-Managed Device

Identity Sources, such as Microsoft AD realms and RADIUS Servers, are AAA servers and databases that define user accounts for the people in your organization. You can use this information in a variety of ways, such as providing the user identity associated with an IP address, or authenticating remote access VPN connections or access to Security Cloud Control.

Click **Objects > FDM Objects**, then click and choose **> RA VPN Objects (ASA & FTD)** > **Identity Source** to create your sources. You would then use these objects when you configure the services that require an identity source. You can apply appropriate filters to search existing sources and manage them.

Active Directory Realms

Active Directory provides user account and authentication information. When you deploy a configuration that includes an AD realm to an FDM-managed device, Security Cloud Control fetches users and groups from the AD server.

You can use this source for the following purposes:

- Remote Access VPN, as a primary identity source. You can use AD in conjunction with a RADIUS server.
- Identity policy, for active authentication and as the user identity source used with passive authentication.
- Identity rule, for active authentication for a user.

You can create access control rules with user identities. See How to Implement an Identity Policy for more information.

Security Cloud Control requests an updated list of user groups once every 24 hours. Because you can add a maximum of 50 users or groups to a rule, selecting groups usually makes more sense than selecting individual users. For example, you could create a rule allowing the Engineering group access to a development network, and create a subsequent rule that denies all other access to the network. Then, to make the rule apply to new engineers, you only need to add the engineer to the Engineering group in the directory server.

Active Directory Realms In Security Cloud Control

You configure the AD realm when you create an AD Identity object. The identity source objects wizard assists in determining how to connect to the AD server and where the AD server is located in the network.

Note If you create an AD realm in Security Cloud Control, Security Cloud Control remembers the AD password when you create affiliate identity source objects and when you add those objects to an identity rule.

Active Directory Realms In FDM

You can point to AD realm objects that were created in FDM from the Security Cloud Control objects wizard. Note that Security Cloud Control does **not** read the AD password for AD realm objects that are created in FDM. You must manually enter the correct AD password in Security Cloud Control.

To configure an AD realm in firewall device managers, see the **Configuring AD Identity Realms** section of the Reusable Objects chapters of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Supported Directory Servers

You can use AD on Windows Server 2008 and 2012.

Note the following about your server configuration:

- If you want to perform user control on user groups or on users within groups, you must configure user groups on the directory server. The system cannot perform user group control if the server organizes the users in a basic object hierarchy.
- The directory server must use the field names listed in the following table in order for the system to retrieve user metadata from the servers for that field:

Metadata	Active Directory Field
LDAP user name	samaccountname
First name	givename
Last Name	sn
email address	mail userprincipalname (if mail has no value)
Department	department distinguishedname (if department has no value)
Telephone number	telephonenumber

Determining the Directory Base DN

When you configure directory properties, you need to specify the common base Distinguished Name (DN) for users and groups. The base is defined in your directory server and differs from network to network. You must enter the correct bases for identity policies to work. If the base is wrong, the system cannot determine user or group names, and thus identity-based policies will be inoperable.

Note To get the correct bases, consult the administrator who is responsible for the directory servers.

For an active directory, you can determine the correct bases by logging into the AD server as a domain administrator, and using the **dsquery** command at a command prompt as follows to determine the bases:

User search base

Enter the **dsquery user** command with known username (partial or complete) to determine the base distinguished name. For example, the following command uses the partial name "John*" to return information for all users that start with "John."

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

The base DN would be "DC=csc-lab,DC=example,DC=com."

Group search base

Enter the **dsquery group** command with a known group name to determine the base DN. For example, the following command uses the group name Employees to return the distinguished name:

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

The group base DN would be "DC=csc-lab,DC=example,DC=com."

You can also use the ADSI Edit program to browse the AD structure (**Start** > **Run** > **adsiedit.msc**). In ADSI Edit, right click any object, such as an organizational unit (OU), group, or user, and choose **Properties** to view the distinguished name. You can then copy the string of DC values as the base.

To verify that you have the correct base:

Procedure

Step 1 Click the **Test Connection** button in the directory properties to verify connectivity. Resolve any problems, and save the directory properties.

Step 2 Commit changes to the device.

Step 3 Create an access rule, select the **Users** tab, and try to add known user and group names from the directory. You should see auto-complete suggestions as you type for matching users and groups in the realm that contains the directory. If these suggestions appear in a drop-down list, then the system was able to query the directory successfully. If you see no suggestions, and you are certain the string you typed should appear in a user or group name, you need to correct the corresponding search base.

What to do next

See Create or Edit an Active Directory Realm Object for more information.

RADIUS Servers and Groups

You can use RADIUS servers to authenticate and authorize administration users.

When you configure a feature to use RADIUS servers, you select a RADIUS group instead of individual servers. A RADIUS group is a collection of RADIUS servers that are copies of each other. If a group has more than one server, they form a chain of backup servers to provide redundancy in case one server becomes unavailable. But even if you have only one server, you must create a one-member group to configure RADIUS support for a feature.

You can use this source for the following purposes:

- Remote Access VPN, as an identity source for authentication, and for authorization and accounting. You can use AD in conjunction with a RADIUS server.
- Identity policy, as a passive identity source to collect user identity from remote access VPN logins.

See Create or Edit a RADIUS Server Object or Group for more information.

Related Information:

- Create or Edit an Active Directory Realm Object
- Create or Edit a RADIUS Server Object or Group
- Configure Identity Policies

Create or Edit an Active Directory Realm Object

About Active Directory Realm Objects

When you create or edit an identity source object such as an AD realm object, Security Cloud Control sends the configuration request to the FDM-managed devices through the SDC. The FDM-managed device then communicates with the configured AD realm.

Note that Security Cloud Control does not read the Directory Password for AD realms that are configured through the firewall device manager console. If you use an AD realm object that was originally created in firewall device manager, you must manually enter the Directory Password.

Create an FTD Active Directory Realm Object

Use the following procedure to create an object:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click  , then click **RA VPN Objects (ASA & FTD)** > **Identity Source**.

Step 3 Enter an **Object Name** for the object.

Step 4 Select the **Device Type** is as **FTD**.

Step 5 In the first part of the wizard, select **Active Directory Realm** as the **Identity Source Type**. Click **Continue**.

Step 6 Configure the basic realm properties.

- **Directory Username, Directory Password** - The distinguished username and password for a user with appropriate rights to the user information you want to retrieve. For AD, the user does not need elevated privileges. You can specify any user in the domain. The username must be fully qualified; for example, Administrator@example.com (not simply Administrator).

  Note The system generates ldap-login-dn and ldap-login-password from this information. For example, Administrator@example.com is translated as cn=administrator,cn=users,dc=example,dc=com. Note that cn=users is always part of this translation, so you must configure the user you specify here under the common name "users" folder.

- **Base Distinguished Name** - The directory tree for searching or querying user and group information, that is, the common parent for users and groups. For example, cn=users,dc=example,dc=com.
- **AD Primary Domain** - The fully qualified AD domain name that the device should join. For example, example.com.

Step 7 Configure the directory server properties.

- **Hostname/IP Address** - The hostname or IP address of the directory server. If you use an encrypted connection to the server, you must enter the fully-qualified domain name, not the IP address.
- **Port** - The port number used for communications with the server. The default is 389. Use port 636 if you select LDAPS as the encryption method.
- **Encryption** - To use an encrypted connection for downloading user and group information, select the desired method,**STARTTLS** or **LDAPS**. The default is **None**, which means that user and group information is downloaded in clear text.
  - **STARTTLS** negotiates the encryption method and uses the strongest method supported by the directory server. Use port 389. This option is not supported if you use the realm for remote access VPN.
  - **LDAPS** requires LDAP over SSL. Use port 636.
- **Trusted CA Certificate** - If you select an encryption method, upload a Certificate Authority (CA) certificate to enable a trusted connection between the system and the directory server. If you are using a certificate to authenticate, the name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.

Step 8 (Optional) Use the **Test** button to validate the configuration.

Step 9 (Optional) Click **Add another configuration** to add multiple AD servers to the AD realm. The AD servers need to be duplicates of each other and support the same AD domain. Therefore, the basic realm properties such as **Directory name**, **Directory Password**, and **Base Distinguished Name** must be the same across all AD servers associated with that AD realm.

Step 10 Click **Add**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit an FTD Active Directory Realm Object

Note that you cannot change the Identity Source Type when editing an Identity source object. You must create a new object with the correct type.

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon  in the **Actions** pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created in the procedures above. Expand the configuration bar listed below to edit or test the hostname/IP address or encryption information.

Step 6 Click **Save**.

Step 7 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Create or Edit a RADIUS Server Object or Group
- Configure Identity Policies
- Configure Identity Rules
- Configure Identity Policy Settings

Create or Edit a RADIUS Server Object or Group

About RADIUS Server Objects or Groups

When you create or edit an identity source object such as a RADIUS server object or a group of RADIUS server objects, Security Cloud Control sends the configuration request to the FDM-managed devices through the SDC. The FDM-managed device then communicates with the configured AD realm.

Create a RADIUS Server Object

RADIUS servers provide AAA (authentication, authorization, and accounting) services.

Use the following procedure to create an object:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click  , then click **RA VPN Objects (ASA & FTD)** > **Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 For the **Device Type**, select **FTD**.

Step 5 For the **Identity Source** type, select **RADIUS Server**. Click **Continue**.

Step 6 Edit the Identity Source configuration with the following properties:

- **Server Name or IP Address** - The fully-qualified host name (FQDN) or IP address of the server.
- **Authentication Port** (Optional) - The port on which RADIUS authentication and authorization are performed. The default is 1812.
- **Timeout** - The length of time, 1-300 seconds, that the system waits for a response from the server before sending the request to the next server. The default is 10 seconds.
- Enter the **Server Secret Key**(Optional) - The shared secret that is used to encrypt data between the Firepower Threat Defense device and the RADIUS server. The key is a case-sensitive, alphanumeric string of up to 64 characters, with no spaces. The key must start with an alphanumeric character or an underscore, and it can contain the special characters: $ & - _ . + @. The string must match the one configured on the RADIUS server. If you do not configure a secret key, the connection is not encrypted.

Step 7 If you have Cisco Identity Services Engine (ISE) already configured for your network and are using the server for remote access VPN Change of Authorization configuration, click the **RA VPN Only** link and configure the following:

- **Redirect ACL** - Select the extended Access Control List (ACL) to use for the RA VPN redirect ACL. If you do not have an extended ACL you must create the required extended ACL object from a Smart CLI template in the FDM-managed device console. See the **Configuring Smart CLI Objects** section of the Advanced Configuration chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running. The purpose of the redirect ACL is to send initial traffic to ISE to assess the client posture. The ACL should send HTTPS traffic to ISE, but not traffic that is already destined for ISE, or traffic that is directed to a DNS server for name resolution. See the **Configure Change of Authorization** section of the Virtual Private Networks (VPN) chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Managerfor the version your device is running.
- **Diagnostic Interface** -Enabling this option allows the system to always use the "Diagnostic" interface to communicate with the server. If you leave this disabled, Security Cloud Control will default to using the routing table to determine the which interface to use.

Step 8 Click **Add**.

Step 9 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create a RADIUS Server Group

A RADIUS server group contains one or more RADIUS server objects. The servers within a group must be copies of each other. These servers form a chain of backup servers, so that if the first server is unavailable, the system can try the next server in the list.

Use the following procedure to create an object group:

Procedure

Step 1 In the left pane, click **Objects > FDM Objects**.

Step 2 Click  , then click **FTD** > **Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 Select the **Device Type** as **FTD**.

Step 5 Select **RADIUS Server Group** as the Identity Source Type. Click **Continue**.

Step 6 Edit the Identity Source configuration with the following properties:

- **Dead Time** - Failed servers are reactivated only after all servers have failed. The dead time is how long to wait after the last server fails before reactivating all servers.
- **Maximum Failed Attempts** - The number of failed requests (that is, requests that do not get a response) sent to a RADIUS server in the group before trying the next server. When the maximum number of failed attempts is exceeded, the system marks the server as Failed. For a given feature, if you configured a fallback method using the local database, and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for the duration of the dead time, so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately.
- **Dynamic Authorization/Port** (Optional) - If you enable RADIUS dynamic authorization or change of authorization (CoA) services for this RADIUS server group, the group will be registered for CoA notification and listen on the specified port for CoA policy updates from Cisco Identity Services Engine (ISE). Enable dynamic authorization only if you are using this server group in a remote access VPN in conjunction with ISE.

Step 7 Select an AD realm that supported the RADIUS server from the drop-down menu. If you have not already created an AD realm, click **Create** from inside the drop-down menu.

Step 8 Click the **Add** button  to add existing RADIUS server objects. Optionally, you can create a new RADIUS server object from this window is necessary.

Note Add these objects in priority, as the first server in the list is used until it is unresponsive. FDM-managed device then defaults to the next server in the list.

Step 9 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit a Radius Server Object or Group

Use the following procedure to edit a Radius server object or Radius server group:

Procedure

Step 1 In the left pane, click **Objects** > **FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon in the **Actions** pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above. To edit or test the hostname/IP address or encryption information, expand the configuration bar.

Step 6 Click **Save**.

Step 7 Security Cloud Control displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create New RA VPN Group Policies

A group policy is a set of user-oriented attribute/value pairs for remote access VPN connections. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

The system includes a default group policy named "DfltGrpPolicy". You can create additional group policies to provide the services you require.

Note You cannot add inconsistent group policy objects to RA VPN configuration. Resolve all inconsistencies before adding the group policy to the RA VPN Configuration.

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FTD)** > **RA VPN Group Policy**.

Step 4 Enter a name for the group policy. The name can be up to 64 characters and spaces are allowed.

Step 5 In the **Device Type** drop-down, select **FTD**.

Step 6 Do any of the following:

- Click the required tabs and configure the attributes on the page:
  - RA VPN Group Policy Attributes
  - AnyConnect Client Profiles, on page 483

- Session Setting Attributes, on page 484
- Address Assignment Attributes, on page 485
- Split Tunneling Attributes, on page 485
- AnyConnect Attributes, on page 486
- Traffic Filters Attributes, on page 487
- Windows Browser Proxy Attributes, on page 488

Step 7 Click **Save** to create the group policy.

RA VPN Group Policy Attributes

The general attributes of a group policy define the name of the group and some other basic settings. The Name attribute is the only required attribute.

- **DNS Server**: Select the DNS server group that defines the DNS servers clients should use for domain name resolution when connected to the VPN. If the group you need is not yet defined, click **Create DNS Group** and create it now.
- **Banner**: The banner text, or welcome message, to present to users at login. The default is no banner. The length can be up to 496 characters. The AnyConnect client supports partial HTML. To ensure that the banner displays properly to remote users, use the <BR> tag to indicate line breaks.
- **Default Domain**: The default domain name for users in the RA VPN. For example, example.com. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.
- **AnyConnect Client Profiles**: Click + and select the AnyConnect Client Profiles to use for this group. See Upload RA VPN AnyConnect Client Profile. If you configure a fully-qualified domain name for the outside interface (in the connection profile), a default profile will be created for you. Alternatively, you can upload your client profile. Create these profiles using the Standalone AnyConnect Profile Editor, which you can download and install from software.cisco.com. If you do not select a client profile, the AnyConnect client uses default values for all options. The items in this list are AnyConnect Client Profile objects rather than the profiles themselves. You can create (and upload) new profiles by clicking **Create New AnyConnect Client Profile** in the drop-down list.

AnyConnect Client Profiles

This feature is supported on firewall device manager running software version 6.7 or later versions.

Cisco AnyConnect VPN client offers enhanced security through various built-in modules. These modules provide services such as web security, network visibility into endpoint flows, and off-network roaming protection. Each client module includes a client profile that includes a group of custom configurations as per your requirement.

You can select the AnyConnect VPN profile object and AnyConnect modules to be downloaded to clients when the VPN user downloads the VPN AnyConnect client software.

1. Choose or create an AnyConnect VPN profile object. See Upload RA VPN AnyConnect Client Profile, on page 499. Except for DART and Start Before Login modules, the AnyConnect VPN profile object must be selected.
2. Click **Add Any Connect Client Module**.

   The following AnyConnect modules are optional and you can configure these modules to be downloaded with VPN AnyConnect client software:

   - **AMP Enabler** — Deploys advanced malware protection (AMP) for endpoints.
   - **DART** — Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
   - **Feedback** — Provides information about the features and modules customers have enabled and used.
   - **ISE Posture** — Uses the OPSWAT library to perform posture checks to assess an endpoint's compliance.
   - **Network Access Manager** — Provides 802.1X (Layer 2) and device authentication to access both wired and wireless networks.
   - **Network Visibility** — Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics.
   - **Start Before Login** — Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.
   - **Umbrella Roaming Security** — Provides DNS-layer security when no VPN is active.
   - **Web Security** — Analyzes the elements of a web page, allows acceptable content, and blocks malicious or unacceptable content based on a defined security policy.
3. In the **Client Module** list, select an **AnyConnect module**.
4. In the **Profile** list, choose or create a profile object containing an AnyConnect Client Profile.
5. Select **Enable Module Download** to enable endpoints to download the client module along with the profile. If not selected, the endpoints can download only the client profile.

Session Setting Attributes

The session settings of a group policy control how long users can connect through the VPN and how many separate connections they can establish.

- **Maximum Connection Time**: The maximum length of time, in minutes, that users can stay connected to the VPN without logging out and reconnecting, from 1- 4473924 or blank. The default is unlimited (blank), but the idle timeout still applies.
- **Connection Time Alert Interval**: If you specify a maximum connection time, the alert interval defines the amount of time before the maximum time is reached to display a warning to the user about the upcoming automatic disconnect. The user can choose to end the connection and reconnect to restart the timer. The default is 1 minute. You can specify 1 to 30 minutes.

- **Idle Time**: The length of time, in minutes, that the VPN connection can be idle before it is automatically closed, from 1-35791394. If there is no communication activity on the connection for this consecutive number of minutes, the system stops the connection. The default is 30 minutes.
- **Idle Time Alert Interval**: The amount of time before the idle time is reached to display a warning to the user about the upcoming automatic disconnect due to an idle session. Any activity resets the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Simultaneous Login Per User**: The maximum number of simultaneous connections allowed for a user. The default is 3. You can specify 1 to 2147483647 connections. Allowing many simultaneous connections might compromise security and affect performance.

Address Assignment Attributes

The address assignment attributes of a group policy define the IP address pool for the group. The pool defined here overrides the pool defined in any connection profile that uses this group. Leave these settings blank if you want to use the pool defined in the connection profile.

- **IPv4 Address Pool, IPv6 Address Pool**: These options define the address pools for the remote endpoints. Clients are assigned an address from these pools based on the IP version they use to make the VPN connection. Select a network object that defines a subnet for each IP type you want to support. Leave the list empty if you do not want to support that IP version. For example, you could define an IPv4 pool as 10.100.10.0/24. The address pool cannot be on the same subnet as the IP address for the outside interface. You can specify a list of up to six address pools to use for local address allocation. The order in which you specify the pools is significant. The system allocates addresses from these pools in the order in which the pools appear.
- **DHCP Scope**: If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same pool identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group. If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address. To specify a scope, select the network object that contains the network number host address. Click **Create New Network** if the object does not yet exist. For example, to tell the DHCP server to use addresses from the 192.168.5.0/24 subnet pool, select a network object that specifies 192.168.5.0 as a host address. You can use DHCP for IPv4 addressing only.

Split Tunneling Attributes

The split tunneling attributes of a group policy define how the system should handle traffic meant for the internal network vs. externally-directed traffic. Split tunneling directs some network traffic through the VPN tunnel (encrypted) and the remaining network traffic outside the VPN tunnel (unencrypted or in clear text).

- **IPv4 Split Tunneling**, **IPv6 Split Tunneling**: You can specify different options based on whether the traffic uses IPv4 or IPv6 addresses, but the options for each are the same. If you want to enable split tunneling, specify one of the options that require you to select network objects.
  - **Allow all traffic over tunnel**: Do no split tunneling. Once the user makes an RA VPN connection, all the user's traffic goes through the protected tunnel. This is the default. It is also considered the most secure option.
  - **Allow specified traffic over the tunnel**: Select the network objects that define destination network and host addresses. Any traffic to these destinations goes through the protected tunnel. The client

routes traffic to any other destination to connections outside the tunnel (such as a local Wi-Fi or network connection).

- **Exclude networks specified below**: Select the network objects that define destination network or host addresses. The client routes any traffic to these destinations to connections outside the tunnel. Traffic to any other destination goes through the tunnel.

- **Split DNS** - You can configure the system to send some DNS requests through the secure connection while allowing the client to send other DNS requests to the DNS servers configured on the client. You can configure the following DNS behavior:
  - **Send DNS Request as per split tunnel policy**: With this option, DNS requests are handled the same way as the split tunnel options are defined. If you enable split tunneling, DNS requests are sent based on the destination addresses. If you do not enable split tunneling, all DNS requests go over the protected connection.
  - **Always send DNS requests over tunnel**: Select this option if you enable split tunneling, but you want all DNS requests sent through the protected connection to the DNS servers defined for the group.
  - **Send only specified domains over tunnel**: Select this option if you want your protected DNS servers to resolve addresses for certain domains only. Then, specify those domains, separating domain names with commas. For example, example.com, example1.com. Use this option if you want your internal DNS servers to resolve names for internal domains, while external DNS servers handle all other Internet traffic.

AnyConnect Attributes

The AnyConnect attributes of a group policy define some SSL and connection settings used by the AnyConnect client for a remote access VPN connection.

- **SSL Settings**
  - **Enable Datagram Transport Layer Security (DTLS)**: Whether to allow the AnyConnect client to use two simultaneous tunnels: an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL tunnel only.
  - **DTLS Compression**: Whether to compress Datagram Transport Layer Security (DTLS) connections for this group using LZS. DTLS Compression is disabled by default.
  - **SSL Compression**: Whether to enable data compression, and if so, the method of data compression to use, **Deflate**, or **LZS**. SSL Compression is **Disabled** by default. Data compression speeds up transmission rates but also increases the memory requirement and CPU usage for each user session. Therefore, SSL compression decreases the overall throughput of the device.
  - **SSL Rekey Method**, **SSL Rekey Interval**: The client can rekey the VPN connection, renegotiating the crypto keys and initialization vectors, to increase the security of the connection. Disable rekeying by selecting **None**. To enable rekey, select **New Tunnel** to create a new tunnel each time. (The **Existing Tunnel** option results in the same action as **New Tunnel**.) If you enable rekeying, also set the rekey interval, which is 4 minutes by default. You can set the interval to 4-10080 minutes (1 week).

- **Connection Settings**
  - **Ignore the DF (Don't Fragment) bit**: Whether to ignore the Don't Fragment (DF) bit in packets that need fragmentation. Select this option to allow the forced fragmentation of packets that have the DF bit set, so that these packets can pass through the tunnel.
  - **Client Bypass Protocol** - Allows you to configure how the secure gateway manages IPv4 traffic (when it is expecting only IPv6 traffic), or how it manages IPv6 traffic (when it is expecting only IPv4 traffic).

    When the AnyConnect client makes a VPN connection to the headend, the headend assigns it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the headend assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can configure the Client Bypass Protocol to drop network traffic for which the headend did not assign an IP address (default, disabled, not checked), or allow that traffic to bypass the headend and be sent from the client unencrypted or "in the clear" (enabled, checked).

    For example, assume that the secure gateway assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual-stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.
  - **MTU**: The maximum transmission unit (MTU) size for SSL VPN connections established by the Cisco AnyConnect VPN Client. The default is 1406 bytes. The range is 576 to 1462 bytes.
    - **Keepalive Messages Between AnyConnect and VPN Gateway**: Whether to exchange keepalive messages between peers to demonstrate that they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals. The default interval is 20 seconds, and the valid range is 15 to 600 seconds.
    - **DPD on Gateway Side Interval**, **DPD on Client Side Interval**: Enable Dead Peer Detection (DPD) to ensure that the VPN gateway or VPN client quickly detects when the peer is no longer responding. You can separately enable gateway or client DPD. The default interval is 30 seconds for sending DPD messages. The interval can be 5-3600 seconds.

Traffic Filters Attributes

The traffic filter attributes of a group policy define restrictions you want to place on users assigned to the group. You can use these attributes instead of creating access control policy rules to restrict RA VPN users to specific resources, based on host or subnet address and protocol, or VLAN. By default, RA VPN users are not restricted by the group policy from accessing any destination on your protected network.

- **Access List Filter**: Restrict access using an extended access control list (ACL). Select the Smart CLI Extended ACL object. The extended ACL lets you filter based on source address, a destination address, and protocol (such as IP or TCP). ACLs are evaluated on a top-down, first-match basis, so ensure that you place specific rules before more general rules. There is an implicit "deny any" at the end of the ACL, so if you intend to deny access to a few subnets while allowing all other access, ensure that you include a "permit any" rule at the end of the ACL. Because you cannot create network objects while editing an extended ACL Smart CLI object, you should create the ACL before editing the group policy. Otherwise, you might need to simply create the object, then go back later to create the network objects and then all the access control entries that you need. To create the ACL, log in to firewall device manager, go to **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**, create an object, and select **Extended Access List** as the object type.

- **Restrict VPN to VLAN**: Also called "VLAN mapping," this attribute specifies the egress VLAN interface for sessions to which this group policy applies. The system forwards all traffic from this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using an ACL to filter traffic on a session. Ensure that you specify a VLAN number that is defined on a subinterface on the device. Values range from 1 to 4094.

Windows Browser Proxy Attributes

The Windows browser proxy attributes of a group policy determine how, and whether, a proxy defined on the user's browser operates.

You can select one of the following values for **Browser Proxy During VPN Session**:

- **No change in endpoint settings**: Allow the user to configure (or not configure) a browser proxy for HTTP and use the proxy if it is configured.
- **Disable browser proxy**: Do not use the proxy defined for the browser, if any. No browser connections will go through the proxy.
- **Auto detect settings**: Enable the use of automatic proxy server detection in the browser for the client device.
- **Use custom settings**: Define a proxy that should be used by all client devices for HTTP traffic. Configure the following settings:
  - **Proxy Server IP or Hostname**, **Port**: The IP address, or hostname, of the proxy server, and the port used for proxy connections by the proxy server. The host and port combined cannot exceed 100 characters.
  - **Browser Proxy Exemption List**: Connections to the hosts/ports in the exemption list do not go through the proxy. Add all the host/port values for destinations that should not use the proxy. For example, www.example.com port 80. Click **Add proxy exemption** to add items to the list. Click the trash can icon to delete items. The entire proxy exception list, combining all addresses and ports, cannot be longer than 255 characters.

Create an RA VPN Configuration

Security Cloud Control allows you to add one or more FDM-managed devices to the RA VPN configuration wizard and configure the VPN interfaces, access control, and NAT exemption settings associated with the devices. Therefore, each RA VPN configuration can have connection profiles and group policies shared across multiple FDM-managed devices that are associated with the RA VPN configuration. Further, you can enhance the configuration by creating connection profiles and group policies.

You can either onboard an FDM-managed device that has already been configured with RA VPN settings or a new device without RA VPN settings. When you onboard an FDM-managed device that already has RA VPN settings, Security Cloud Control automatically creates a "Default RA VPN Configuration" and associates the FDM-managed device with this configuration. Also, this default configuration can contain all the connection profile objects that are defined on the device.

Important

- You are not allowed to add ASA and FDM-managed device in the same Remote Access VPN Configuration.
- An FDM-managed device can't have more than one RA VPN Configuration.

Prerequisites

Before adding the FDM-managed devices to RA VPN configuration, the following prerequisites must be met:

- Make sure that the FDM-managed devices have the following:
  - A valid license. For more information, see Licensing Requirements for Remote Access VPN.
  - For FDM Version 6.4.0, ensure that a minimum of one AnyConnect software package pre-uploaded to the device. For more information, see Upgrade AnyConnect Package on an FDM-Managed Device Running Version 6.4.0.
  - For FDM Version 6.5.0 and later, you can upload AnyConnect package using Security Cloud Control. For more information, see Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later.
  - There are no configuration deployments pending.
- FDM changes are synchronized to Security Cloud Control.
  1. In the left pane, click **Inventory** and search for one or more FDM-managed devices to be synchronized.
  2. Select one or more devices and then click **Check for changes**. Security Cloud Control communicates with one or more FDM-managed devices to synchronize the changes.
- RA VPN configuration group policy objects are consistent.
  - Ensure that all inconsistent group policy objects are resolved as they cannot be added to the RA VPN configuration. Either address the issue or remove inconsistent group policy objects from the **Objects** page. For more information see, Resolve Duplicate Object Issues and Resolve Inconsistent Object Issues.
- RA VPN group policies of the FDM-managed device match RA VPN configuration group policies.

Procedure

Procedure

Step 1 In the left pane, click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**.

Step 2 Click the blue plus button to create a new RA VPN configuration.

Step 3 Enter a name for the Remote Access VPN configuration.

Step 4 Click the blue plus button to add FDM-managed devices to the configuration. You can add the device details and configure network traffic-related permissions that are associated with the device.

a. Provide the following device details:

- **Device**: Select an FDM-managed device that you want to add and click **Select**.

  Important You are not allowed to add ASA and FDM-managed device in the same Remote Access VPN Configuration.

- **Certificate of Device Identity**: Select the internal certificate used for establishing the identity of the device. This establishes the device identity for AnyConnect clients when they make a connection to the device. Clients must accept this certificate to complete a secure VPN connection. If you do not already have a certificate, click **Create New Internal Certificate** in the drop-down list. See Generating Self-Signed Internal and Internal CA Certificates.
- **Outside Interface**: The interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile. To create a new subinterface, see Configure Firepower VLAN Subinterfaces and 802.1Q Trunking.
- **Fully Qualified Domain Name or IP for the Outside Interface**: The name of the interface, for example, ravpn.example.com or the IP address must be provided. If you specify a name, the system can create a client profile for you. **Note**: You are responsible for ensuring that the DNS servers used in the VPN and by clients can resolve this name to the outside interface's IP address. Add the FQDN to the relevant DNS servers.

b. Click **Continue** to configure the traffic permissions.

- **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**: Decrypted traffic is subjected to Access Control Policy inspection by default. Enabling this option bypasses the decrypted traffic option bypasses the access control policy inspection, but the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic. Note that if you select this option, the system configures the sysopt connection permit-vpn command, which is a global setting. This will also impact the behavior of site-to-site VPN connections. If you do not select this option, it might be possible for external users to spoof IP addresses in your remote access VPN address pool, and thus gain access to your network. This can happen because you will need to create access control rules that allow your address pool to have access to internal resources. If you use access control rules, consider using user specifications to control access, rather than source IP address alone. The downside of selecting this option is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections.
- **NAT Exempt**: Enable NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. If you do not exempt VPN traffic from NAT, ensure that the existing NAT rules for the outside and inside interfaces do not apply to the RA VPN pool of addresses. NAT exempt rules are manual static identity NAT rules for a given source/destination interface and network combination, but they are not reflected in the NAT policy, they are hidden. If you enable NAT Exempt, you must also configure the following.
  - **Inside Interfaces**: Select the interfaces for the internal networks remote users will be accessing. NAT rules are created for these interfaces.
  - **Inside Networks**: Select the network objects that represent internal networks remote users will be accessing. The networks list must contain the same IP types as the address pools you are supporting.

Step 5 Click **OK**.

- If you have onboarded an firewall device manager Version 6.4.0 device, the **AnyConnect Packages Detected** shows the AnyConnect packages available in the device.
- If you have onboarded an firewall device manager Version 6.5.0 or later device, you must add the AnyConnect packages from the server where the AnyConnect packages are pre-uploaded. See Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later for instructions.

Step 6 Click **OK**. The device is added to the configuration.

What to do next

Note Select a configuration and under **Actions**, click the appropriate action:

- **Group Policies** to add or remove group policies.
  - Click + to select the required group policies. To create a new RA VPN group policy, see Create New RA VPN Group Policies.
- **Remove** to delete the selected RA VPN configuration.

Modify RA VPN Configuration

You can modify the name and the device details of an existing RA VPN configuration.

Procedure

Select the configuration to be modified and under **Actions**, click **Edit**.

- Modify the name if required.
- Click the blue plus button to add a new device
- Click to perform the following on the FDM-managed device.
  - Click **Edit** to modify the existing RA VPN configuration.
  - Click **Remove** to remove the FDM-managed device from the RA VPN configuration. All connection profiles and RA VPN settings associated with that device except the group policies are deleted. You can remove the group policies explicitly from the objects page. **Note**: You cannot remove the FDM-managed device if that is the only device using the configuration. Alternatively, you can remove the RA VPN configuration.

You can also search for remote access VPN configuration by typing the name of the configuration or device.

Related Information:

- Configure an RA VPN Connection Profile.
- Preview and Deploy Configuration Changes for All Devices.
- Allow Traffic Through the Remote Access VPN.

Configure an RA VPN Connection Profile

An RA VPN connection profile defines the characteristics that allow external users to create a VPN connection to the system using the AnyConnect client. Each profile defines the AAA servers and certificates used for authenticating users, the address pool for assigning users IP addresses, and the group policies that define various user-oriented attributes.

You can create multiple profiles within the RA VPN configuration if you need to provide variable services to different user groups, or if you have various authentication sources. For example, if your organization merges with a different organization that uses different authentication servers, you can create a profile for the new group that uses those authentication servers.

An RA VPN connection profile allows your users to connect to your inside networks when they are on external networks, such as their home network. Create separate profiles to accommodate different authentication methods.

Before you begin

Before configuring the remote access (RA) VPN connection:

- The outside interface, the one that terminates remote access VPN connections, cannot also have a management access list that allows HTTPS connections. Delete any HTTPS rules from the outside interface before configuring RA VPN. See the "Configuring the Management Access List" section in the "System Settings" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version X.Y.
- Create an RA VPN configuration. See Create an RA VPN Configuration.

Procedure

Procedure

Step 1 In the left pane, click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**. You can click a VPN configuration to view the summary information on how many connection profiles and group policies are currently configured.

Step 2 Click the connection profile and under **Actions** in the sidebar at the right, click **Add Connection Profile**.

Step 3 Configure the basic connection attributes.

- **Connection Profile Name**: The name for this connection, up to 50 characters without spaces. For example, MainOffice.

  Note The name you enter here is what users will see in the connection list in the AnyConnect client. Choose a name that will make sense to your users.

- **Group Alias, Group URL**: Aliases contain alternate names or URLs for a specific connection profile. VPN users can choose an alias name in the AnyConnect client in the list of connections when they connect to the FDM-managed device. The connection profile name is automatically added as a group alias. You can also configure the list of group URLs, which your endpoints can select while initiating the Remote Access VPN connection. If users connect using the group URL, the system will automatically use the connection profile that matches the URL. This URL would be used by clients who do not yet have the AnyConnect client installed. Add as many group aliases and URLs as required. These aliases and URLs must be unique across all connection profiles defined on the device. Group URLs must start with **https://**.
- For example, you might have the alias Contractor and the group URLhttps://ravpn.example.com/contractor. Once the AnyConnect client is installed, the user would simply select the group alias in the AnyConnect VPN drop-down list of connections.

Step 4 Configure the primary and optionally, secondary identity sources. These options determine how remote users authenticate to the device to enable the remote access VPN connection. The simplest approach is to use AAA only and then select an AD realm or use the LocalIdentitySource. You can use the following approaches for **Authentication Type**:

- **AAA Only**: Authenticate and authorize users based on username and password. For details, see Configure AAA for a Connection Profile.
- **Client Certificate Only**: Authenticate users based on client device identity certificate. For details, see Configure Certificate Authentication for a Connection Profile.
- **AAA and ClientCertificate**: Use both username/password and client device identity certificate.

Step 5 Configure the address pool for clients. The address pool defines the IP addresses that the system can assign to remote clients when they establish a VPN connection. For more information, see Configure Client Address Pool Assignment.

Step 6 Click **Continue**.

Step 7 Select the **Group Policy** to use for this profile from the list and click **Select**. The group policy sets terms for user connections after the tunnel is established. The system includes a default group policy named DfltGrpPolicy. You can create additional group policies to provide the services you require.

Note If the group policy you need does not yet exist, create the group policy on the **Objects** page and then associate the policy to the RA VPN configuration. For detailed information about group policies, see Create New RA VPN Group Policies.

Step 8 Click **Continue**.

Step 9 Review the summary. First, verify that the summary is correct. You can see what end-users need to do to initially install the AnyConnect software and test that they can complete a VPN connection. Click  to copy the instructions to the clipboard, and then distribute them to your users.

Step 10 Click **Done**.

What to do next

Ensure that traffic is allowed in the VPN tunnel, as explained in Allow Traffic Through the Remote Access VPN.

Configure AAA for a Connection Profile

Authentication, Authorization, and Accounting (AAA) servers use username and password to determine if a user is allowed access to the remote access VPN. If you use RADIUS servers, you can distinguish authorization levels among authenticated users, to provide differential access to protected resources. You can also use RADIUS accounting services to keep track of usage.

When configuring AAA, you must configure a primary identity source. Secondary and fallback sources are optional. Use a secondary source if you want to implement dual authentication, for example, using RSA tokens or DUO.

Primary Identity Source Options

- **Primary Identity Source for User Authentication**: The primary identity source used for authenticating remote users. End users must be defined in this source or the optional fallback source to complete a VPN connection. Select one of the following:
  - An Active Directory (AD) identity realm. If the realm you need does not yet exist, click **Create New Identity Realm**.
  - A RADIUS server group.
  - LocalIdentitySource (the local user database): You can define users directly on the device and not use an external server.
- **Fallback Local Identity Source**: If the primary source is an external server, you can select the LocalIdentitySource as a fallback in case the primary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the external server.
- **Strip options**: A realm is an administrative domain. Enabling the following options allows the authentication to be based on the username alone. You can enable any combination of these options. However, you must select both check boxes if your server cannot parse delimiters.
  - **Strip Identity Source Server from Username**: Whether to remove the identity source name from the username before passing the username on to the AAA server. For example, if you select this option and the user enters domain\username as the username, the domain is stripped off from the username and sent to AAA server for authentication. By default, this option is unchecked.
  - **Strip Group from Username**: Whether to remove the group name from the username before passing the username on to the AAA server. This option applies to names given in the username@domain format; the option strips the domain and @ sign. By default, this option is unchecked.

Secondary Identity Source

- **Secondary Identity Source for User Authorization**: The optional second identity source. If the user successfully authenticates with the primary source, the user is prompted to authenticate with the secondary source. You can select an AD realm, RADIUS server group, or the local identity source.
- **Advanced options**: Click the **Advanced** link and configure the following options:
  - **Fallback Local Identity Source for Secondary**: If the secondary source is an external server, you can select the LocalIdentitySource as a fallback in case the secondary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the secondary external server.

- **Use Primary Username for Secondary Login**: By default, when using a secondary identity source, the system will prompt for both username and password for the secondary source. If you select this option, the system prompts for the secondary password only and uses the same username for the secondary source that was authenticated against the primary identity source. Select this option if you configure the same usernames in both the primary and secondary identity sources.
  - **Username for Session Server**: After successful authentication, the username is shown in events and statistical dashboards, is used for determining matches for a user- or group-based SSL decryption and access control rules and is used for accounting. Because you are using two authentication sources, you need to tell the system whether to use the Primary or Secondary username as the user identity. By default, the primary name is used.
  - **Password Type**: How to obtain the password for the secondary server. The default is **Prompt**, which means the user is asked to enter the password. Select **Primary Identity Source Password** to automatically use the password entered when the user authenticated to the primary server. Select **Common Password** to use the same password for every user, then enter that password in the **Common Password** field.
- **Authorization Server**: The RADIUS server group that has been configured to authorize remote access, VPN users. After authentication is complete, authorization controls the services and commands available to each authenticated user. Authorization works by assembling a set of attributes that describe what the user is authorized to perform, their actual capabilities, and restrictions. Were you not to use authorization, authentication alone would provide the same access to all authenticated users. For information on configuring RADIUS for authorization, see Control User Permissions and Attributes Using RADIUS and Group Policies. Note that if the system obtains authorization attributes from the RADIUS server that overlap those defined in the group policy, the RADIUS attributes override the group policy attributes.
- **Accounting Server**: (Optional.) The RADIUS server group to use to account for the remote access VPN session. Accounting tracks the services users are accessing as well as the number of network resources they are consuming. The FDM-managed device reports user activity to the RADIUS server. Accounting information includes when sessions start and stop, usernames, the number of bytes that pass through the device for each session, the service used, and the duration of each session. You can then analyze the data for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

Configure Certificate Authentication for a Connection Profile

Note This section is not applicable for **Authentication Type** as **AAA Only**.

You can use certificates installed on the client device to authenticate remote access VPN connections.

When using client certificates, you can still configure a secondary identity source, fallback source, and authorization and accounting servers. These are AAA options; for details, see Configure an RA VPN Connection Profile.

Following are the certificate-specific attributes. You can configure these attributes separately for primary and secondary identity sources. Configuring a secondary source is optional.

- **Username from Certificate**: Select one of the following:

- **Map Specific Field**: Use the certificate elements in the order of **Primary Field** and **Secondary Field**. The defaults are CN (Common Name) and OU (Organizational Unit). Select the options that work for your organization. The fields are combined to provide the username, and this is the name used in events, dashboards, and for matching purposes in SSL decryption and access control rules.
- **Use entire DN (distinguished name) as username**: The system automatically derives the username from the DN fields. •

- **Advanced options** (not applicable for **Authentication Type** as **Client Certificate Only**): Click the **Advanced** link and configure the following options:
  - **Prefill username from certificate on user login window**: Whether to fill in the username field with the retrieved username when prompting the user to authenticate.
  - **Hide username in login window**: If you select the **Prefill** option, you can hide the username, which means the user cannot edit the username in the password prompt.

Configure Client Address Pool Assignment

There must be a way for the system to provide an IP address to endpoints that connect to the remote access VPN. The AAA server can provide these addresses, a DHCP server, an IP address pool configured in the group policy, or an IP address pool configured in the connection profile. The system tries these resources in that order and stops when it obtains an available address, which it then assigns to the client. Thus, you can configure multiple options to create a failsafe in case of an unusual number of concurrent connections.

Use one or more of the following methods to configure the address pool for a connection profile.

- **IPv4 Address Pool** and **IPv4 Address Pool**: First, create up to six network objects that specify subnets. You can configure separate pools for IPv4 and IPv6. Then, select these objects in the **IPv4 Address Pool** and **IPv6 Address Pool** options, either in the group policy or in the connection profile. You do not need to configure both IPv4 and IPv6, configure the addressing scheme you want to support. You also do not need to configure the pool in both the group policy and the connection profile. The group policy overrides the connection profile settings, so if you configure the pools in the group policy, leave the options empty in the connection profile. Note that the pools are used in the order in which you list them.
- **DHCP Servers**: First, configure a DHCP server with one or more IPv4 address ranges for the RA VPN (you cannot configure IPv6 pools using DHCP). Then, create a host network object with the IP address of the DHCP server. You can then select this object in the **DHCP Servers** attribute of the connection profile. You can configure more than one DHCP server. If the DHCP server has multiple address pools, you can use the **DHCP Scope** attribute in the group policy that you attach to the connection profile to select which pool to use. Create a host network object with the network address of the pool. For example, if the DHCP pool contains 192.168.15.0/24 and 192.168.16.0/24, setting the DHCP scope to 192.168.16.0 will ensure that an address from the 192.168.16.0/24 subnet will be selected.

Allow Traffic Through the Remote Access VPN

You can use one of the following techniques to enable traffic flow in the remote access VPN tunnel.

- Configure the **sysopt connection permit-vpn** command, which exempts traffic that matches the VPN connection from the access control policy. The default for this command is **no sysopt connection permit-vpn**, which means VPN traffic must also be allowed by the access control policy. This is the more secure method to allow traffic in the VPN because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to

the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections. To configure this command, select the **Bypass Access Control policy for decrypted traffic** option in your RA VPN Configuration. See Create an RA VPN Configuration.

- Create access control rules to allow connections from the remote access VPN address pool. This method ensures that VPN traffic is inspected, and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network. See Configure the FDM Access Control Policy.

Upgrade AnyConnect Package on an FDM-Managed Device Running Version 6.4.0

You can use Security Cloud Control to upgrade the AnyConnect package available on an FDM-managed device so that it can be distributed to RA VPN users.

The following are the major steps that are involved in upgrading the AnyConnect package:

Procedure

Step 1 Use firewall device manager to remove the AnyConnect package and upload a later version of the package. Use one of these methods to accomplish this task.

- Remove the old package and upload the new package from the firewall device manager UI.
- Remove the old package and upload the new package from the firewall device manager API explorer.

Step 2 Deploy firewall device manager changes to device.

Step 3 Read the new configuration information into Security Cloud Control.

Step 4 Verify the new package in the RA VPN connection profile.

Prerequisites

- A minimum of one RA VPN configuration with connection profile is already deployed to FDM-managed device.
- Download the AnyConnect package that you want from https://software.cisco.com/download/home/283000185. Cisco recommends upgrading to the latest available package.

Upload your desired AnyConnect Package to Secure Firewall Threat Defense using Firewall Device Manager

Procedure

Step 1 Using a browser, open the home page of the system. For example, https://ftd.example.com.

Step 2 Log into Firewall Device Manager.

Step 3 Click **View Configuration** in the **Device** > **Remote Access VPN** group. The group shows summary information on how many connection profiles and group policies are currently configured.

Step 4 Click the view ( ) button (**View** configuration button.) to open a summary of the connection profile and connection instructions.

Note You can edit any one of the connection profiles to upload the AnyConnect package to the FDM-managed device.

Step 5 Click the **Edit** button to make changes.

Step 6 Click **Next** until the **Global Settings** screen appears. The **AnyConnect Package** shows AnyConnect packages available on the FDM-managed device.

Step 7 Click 'X' button to remove the AnyConnect package which you want to replace.

Step 8 Click **Upload Package** and then click the OS that you want for uploading the compatible package.

Step 9 Select the package and click **Open**. You can see the package being uploaded on the Firewall device manager UI.

Step 10 Click **Finish**. The configuration is saved.

Note Alternatively, you can use the Firewall device manager API explorer to remove and upload a new AnyConnect package.

a. Edit the URL to point to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

b. Delete a package from the FDM-managed device, click **AnyConnectPackageFile** > **Delete**. In the **objID** field, type the package id and click **TRY IT OUT!**.

c. Upload a new package by performing the steps that are described in the Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0 section.

Step 11 Click the **Deploy Changes** icon in the upper right of the web page. The icon is highlighted with a dot when there are undeployed changes.

Step 12 If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately. The window shows that the deployment is in progress. You can close the window, or wait for the deployment to complete.

Verify the new package is referenced in the RA VPN connection profile

Procedure

Step 1 In the left pane, click **Secure Connections** > **Remote Access VPN** > **ASA & FDM**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the FDM-managed device which has the upgraded AnyConnect package. This device would be reporting conflict.

Step 4 Accept the Out-of-band changes to overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration. For more information, see Resolve the Conflict Detected Status

Step 5 View the new AnyConnect package by performing the following:

- Click **VPN** > **Remote Access VPN**.
- Click the RA VPN configuration that is associated with this FDM-managed device.
- Click **Edit** under **Actions**. The new package is displayed under **Devices**.

Upload RA VPN AnyConnect Client Profile

The Remote Access VPN AnyConnect Client Profile is a group of configuration parameters stored in a file. There are different AnyConnect client profiles containing configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, AMP Enabler, ISE posture, Network Visibility, Customer Feedback Experience profiles, Umbrella roaming security, and Web Security.

Security Cloud Control allows uploading of these profiles as objects which can be used in the group policy later.

- **AnyConnect VPN Profile** — AnyConnect client profiles are downloaded to clients along with the VPN AnyConnect client software. These profiles define many client-related options, such as auto-connect on startup and auto-reconnect, and whether the end-user can change the option from the AnyConnect client preferences and advanced settings. Security Cloud Control supports the XML file format.
- **AMP Enabler Service Profile** — The profile is used for the AnyConnect AMP Enabler. The AMP Enabler and this profile are pushed to the endpoints from FDM-managed device when a remote access VPN user connects to the VPN. Security Cloud Control supports XML and ASP file formats.
- **Feedback Profile** — You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and used. Security Cloud Control supports the FSP file format.
- **ISE Posture Profile** — Choose this option if you add a profile file for the AnyConnect ISE Posture module. Security Cloud Control supports XML and ISP file formats.
- **Network Access Manager Service Profile** — Configure and add the NAM profile file using the Network Access Manager profile editor. Security Cloud Control supports XML and NSP file formats.
- **Network Visibility Service Profile** — Profile file for AnyConnect Network Visibility module. You can create the profile using the NVM profile editor. Security Cloud Control supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** — You must select this file type if you deploy the Umbrella Roaming Security module. Security Cloud Control supports XML and JSON file formats.
- **Web Security Service Profile** — Select this file type when you add a profile file for the Web security module. Security Cloud Control supports XML, WSO, and WSP file formats.

Before you begin

Use the suitable GUI-based AnyConnect profile editors to create the profiles you need. You can download the profile editors from Cisco Software Download Center in the AnyConnect Secure Mobility Client category and install the AnyConnect "Profile Editor - Windows / Standalone installer (MSI)." The profile editor installer contains stand-alone versions of the profile editors. The installation file is for Windows only and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect version. For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor.

Except for the Umbrella Roaming Security profile editor, this package contains all the profile editors required for creating the modules. For detailed information, see the *AnyConnect Profile Editor* chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details. Download the Umbrella Roaming Security profile separately from the Umbrella dashboard. For detailed information, see the "Download the AnyConnect Roaming Security Profile from the Umbrella Dashboard" section of the "Umbrella Roaming Security" chapter in the Cisco Umbrella User Guide.

Procedure

Step 1 In the left pane, choose **Objects > FDM Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **AnyConnect Client Profile**.

Step 4 In the **Object Name** field, enter a name for the AnyConnect client profile.

Step 5 Click **Browse** and select the file you created using the Profile Editor.

Step 6 Click **Open** to upload the profile.

Step 7 Click **Add** to add the object.

Related information:

- Associate the client modules with the AnyConnect VPN profile in the RA VPN group policies window. See Create New RA VPN Group Policies.

Note The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Guidelines and Limitations of Remote Access VPN for FDM-Managed Device

Keep the following guidelines and limitations in mind when configuring RA VPN.

- AnyConnect packages must be pre-loaded to FDM-Managed devices running Version 6.4.0 using firewall device manager.

Note Upload AnyConnect package separately to the FDM-Managed device running Version 6.5.0 using the Remote Access VPN Configuration wizard in Cisco Security Cloud Control.

- Before configuring RA VPN from Security Cloud Control:
  - Register the license for the FDM-managed devices from firewall device manager.
  - Enable the license from firewall device manager with export-control.
- Security Cloud Control does not support the Extended Access List object. Configure the object using the Smart CLI in firewall device manager and then use in VPN filter and Change of Authorization (CoA) redirect ACL.
- The template you create from an FDM-managed device will not contain the RA VPN configuration.
- Device-specific overrides are required for IP pool objects and RADIUS identity sources.
- You cannot configure both firewall device manager access (HTTPS access in the management access-list) and AnyConnect remote access SSL VPN on the same interface for the same TCP port. For example, if you configure remote access SSL VPN on the outside interface, you cannot also open the outside interface for HTTPS connections on port 443. Because you cannot configure the port used by these features in firewall device manager, you cannot configure both features on the same interface.
- If you configure two-factor authentication using RADIUS and RSA tokens, the default authentication timeout of 12 seconds is too quick to allow successful authentication in most cases. Increase the authentication timeout value by creating a custom AnyConnect client profile and applying it to the RA VPN connection profile, as described in Upload RA VPN AnyConnect Client Profile, on page 499. We recommend an authentication timeout of at least 60 seconds so that users have enough time to authenticate and then paste the RSA token and for the round-trip verification of the token.

How Users Can Install the AnyConnect Client Software on FDM-Managed Device

Use firewall device manager APIs to upload the AnyConnect Client Software package to FDM-managed device to distribute to your users. See Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0.

To complete a VPN connection, your users must install the AnyConnect client software. You can use your existing software distribution methods to install the software directly. Or, you can have users install the AnyConnect client directly from the FDM-managed device.

Note Users must have Administrator rights on their workstations to install the software.

If you decide to have users initially install the software from the FDM-managed device, inform users to perform the following steps:

Note Android and iOS users should download AnyConnect from the appropriate App Store.

Procedure

Step 1 Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. You identify this interface when you configure the remote access VPN. The system prompts the user to log in.

Step 2 Log into the site. Users are authenticated using the directory server configured for the remote access VPN. Log in must be successful to continue. If the login is successful, the system determines if the user already has the required version of the AnyConnect client. If the AnyConnect client is absent from the user's computer or is down-level, the system automatically starts installing the AnyConnect software. When the installation is finished, AnyConnect completes the remote access VPN connection.

Distribute new AnyConnect Client Software version

You can distribute the new version of AnyConnect client software to your users by uploading them to FDM-managed device without removing the old version. Once the AnyConnect client is uploaded successfully, you can remove the old version.

The AnyConnect client detects the new version on the next VPN connection the user makes. The system will automatically prompt the user to download and install the updated client software. This automation simplifies software distribution for you and your clients.

The following figure shows an example of an FDM-managed device with two versions of AnyConnect client software (**AnyConnectWindows_3.2_BGL** and **AnyConnectWindows_4.2_BGL**) for Windows OS.

Upload RA VPN AnyConnect Client Profile

The Remote Access VPN AnyConnect Client Profile is a group of configuration parameters stored in a file. There are different AnyConnect client profiles containing configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, AMP Enabler, ISE posture, Network Visibility, Customer Feedback Experience profiles, Umbrella roaming security, and Web Security.

Security Cloud Control allows uploading of these profiles as objects which can be used in the group policy later.

- **AnyConnect VPN Profile** — AnyConnect client profiles are downloaded to clients along with the VPN AnyConnect client software. These profiles define many client-related options, such as auto-connect on startup and auto-reconnect, and whether the end-user can change the option from the AnyConnect client preferences and advanced settings. Security Cloud Control supports the XML file format.
- **AMP Enabler Service Profile** — The profile is used for the AnyConnect AMP Enabler. The AMP Enabler and this profile are pushed to the endpoints from FDM-managed device when a remote access VPN user connects to the VPN. Security Cloud Control supports XML and ASP file formats.
- **Feedback Profile** — You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and used. Security Cloud Control supports the FSP file format.
- **ISE Posture Profile** — Choose this option if you add a profile file for the AnyConnect ISE Posture module. Security Cloud Control supports XML and ISP file formats.
- **Network Access Manager Service Profile** — Configure and add the NAM profile file using the Network Access Manager profile editor. Security Cloud Control supports XML and NSP file formats.
- **Network Visibility Service Profile** — Profile file for AnyConnect Network Visibility module. You can create the profile using the NVM profile editor. Security Cloud Control supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** — You must select this file type if you deploy the Umbrella Roaming Security module. Security Cloud Control supports XML and JSON file formats.
- **Web Security Service Profile** — Select this file type when you add a profile file for the Web security module. Security Cloud Control supports XML, WSO, and WSP file formats.

Before you begin

Use the suitable GUI-based AnyConnect profile editors to create the profiles you need. You can download the profile editors from Cisco Software Download Center in the AnyConnect Secure Mobility Client category and install the AnyConnect "Profile Editor - Windows / Standalone installer (MSI)." The profile editor installer contains stand-alone versions of the profile editors. The installation file is for Windows only and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect version. For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor.

Except for the Umbrella Roaming Security profile editor, this package contains all the profile editors required for creating the modules. For detailed information, see the *AnyConnect Profile Editor* chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details. Download the Umbrella Roaming Security profile separately from the Umbrella dashboard. For detailed information, see the "Download the AnyConnect Roaming Security Profile from the Umbrella Dashboard" section of the "Umbrella Roaming Security" chapter in the Cisco Umbrella User Guide.

Procedure

Step 1 In the left pane, choose **Objects** > **FDM Objects**.

Step 2 Click the blue plus  button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **AnyConnect Client Profile**.

Step 4 In the **Object Name** field, enter a name for the AnyConnect client profile.

Step 5 Click **Browse** and select the file you created using the Profile Editor.

Step 6 Click **Open** to upload the profile.

Step 7 Click **Add** to add the object.

Related information:

- Associate the client modules with the AnyConnect VPN profile in the RA VPN group policies window. See Create New RA VPN Group Policies.

Note The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Licensing Requirements for Remote Access VPN

Enable (register) the license for the FDM-managed devices from firewall device manager to configure RA VPN connection. When you register the device, you must do so with a Smart Software Manager (SSM) account that is enabled for export-controlled features. You also cannot configure the feature using the evaluation license.

Also, you must purchase and enable a license; it can be any of the following: . These licenses are treated the same for FDM-managed devices, although they are designed to allow different feature sets when used with ASA Software-based headends.

For more information about enabling license from firewall device manager, see the **Licensing Requirements for Remote Access VPN** section of the Remote Access VPN chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

For more information, see the *Cisco AnyConnect Ordering Guide*. There are also other data sheets available on http://www.cisco.com/c/en/us/product...t-listing.html.

To view the license status, perform the following:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** device.

Step 3 Click the **FTD** tab and select a device that you want.

Step 4 In the **Device Actions** pane on the right, click **Manage Licenses**. If the license is valid, the **Status** shows **Enabled**.

Maximum Concurrent VPN Sessions By Device Model

There is a maximum limit to the number of concurrent remote access VPN sessions allowed on a device based on the device model. This limit is designed, so that system performance does not degrade to unacceptable levels. Use these limits for capacity planning.

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7,500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of authentication, authorization, and accounting (AAA) session after it is authenticated. A key challenge for RA VPNs is to secure the internal network against compromised endpoints and to secure the endpoint itself when it is affected by viruses or malware, by remediating the attack on the endpoint. There is a need to secure the endpoint and the internal network in all phases, that is, before, during, and after the RA VPN session. The RADIUS CoA feature helps in achieving this goal.

If you use Cisco Identity Services Engine (ISE) RADIUS servers, you can configure Change of Authorization policy enforcement. When a policy changes for a user or user group in AAA, ISE sends CoA messages to the FDM-managed device to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is not required to apply access control lists (ACLs) for each VPN session established with the FDM-managed device.

Related Information:

- Configure Change of Authorization on the FDM-Managed Device

Configure Change of Authorization on the FDM-Managed Device

Most of the Change of Authorization policy is configured in the ISE server. However, you must configure the FDM-managed device to connect to ISE correctly.

Before you begin

If you use hostnames in any object, ensure that you configure DNS servers for use with the data interfaces, as explained in **Configuring DNS for Data and Management Interfaces** section of the System Settings chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.You typically need to configure DNS anyway to have a fully-functional system.

Procedure

Procedure

Step 1 Log in to the firewall device manager for your FDM-managed device.

Step 2 Configure the extended access control list (ACL) for redirecting initial connections to ISE. The purpose of the redirect ACL is to send initial traffic to ISE so that ISE can assess the client posture. The ACL should send HTTPS traffic to ISE, but not traffic that is already destined for ISE, or traffic that is directed to a DNS server for name resolution. A sample redirect ACL might look like the following:

access-list redirect extended deny ip any host <ISE server IP>

access-list redirect extended deny ip any host <DNS server IP>

access-list redirect extended deny icmp any any

access-list redirect extended permit tcp any any eq www

However, note that ACLs have an implicit "deny any any" as the last access control entry (ACE). In this example, the last ACE, which matches TCP port www (that is, port 80), will not match any traffic that matches the first 3 ACEs, so those are redundant. You could simply create an ACL with the last ACE and get the same results. Note that in a redirect ACL, the permit and deny actions simply determine which traffic matches the ACL, with permit matching and deny not matching. No traffic is actually dropped, denied traffic is simply not redirected to ISE. To create the redirect ACL, you need to configure a Smart CLI object.

a. Choose **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**.

b. Click **+** to create a new object.

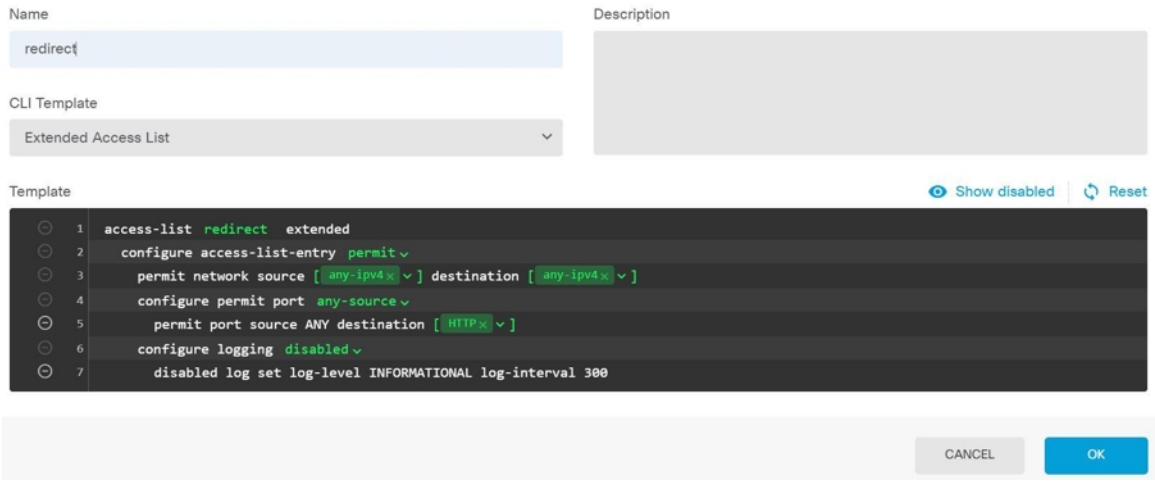
c. Enter a name for the ACL. For example, **redirect**.

d. For **CLI Template**, select **Extended Access List**.

e. Configure the following in the **Template** body:

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source
- destination-port = HTTP
- configure logging = disabled

The ACE should look like the following:



f. Click **OK**.

This ACL will be configured the next time you deploy changes. You do not need to use the object in any other policy to force deployment.

Note This ACL applies to IPv4 only. If you also want to support IPv6, simply add a second ACE with all the same attributes, except select any-ipv6 for the source and destination networks. You can also add the other ACEs to ensure traffic to the ISE or DNS server is not redirected. You will first need to create host network objects to hold the IP addresses of those servers.

Step 3 Configure a RADIUS server group for dynamic authorization.

Perform the below steps by following the instructions provided in the Create or Edit a RADIUS Server Object or Group section.

a. Create a RADIUS Server Object

b. Create a RADIUS Server Group

Step 4 Create a connection profile that uses this RADIUS server group. See Configure an RA VPN Connection Profile. Use **AAA Authentication** (either only or with certificates), and select the server group in the **Primary Identity Source for User Authentication**, **Authorization**, and **Accounting** options.

Verify Remote Access VPN Configuration of FDM-Managed Device

After you configure the remote access VPN and deploy the configuration to the device, verify that you can make remote connections.

Procedure

Step 1 From an external network, establish a VPN connection using the AnyConnect client. Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. If necessary, install the client software and complete the connection. See How Users Can Install the AnyConnect Client Software on FDM-Managed Device. If you configured group URLs, also try those URLs.

Step 2 In the **Inventory** page, select the device you want to verify and click **Command Line Interface** under **Device Actions**.

Step 3 Use the **show vpn-sessiondb** command to view summary information about current VPN sessions.

Step 4 The statistics should show your active AnyConnect Client session, and information on cumulative sessions, the peak concurrent number of sessions, and inactive sessions. Following is sample output from the command.

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                          Active : Cumulative : Peak Concur : Inactive
                         ------------------------------------------------
AnyConnect Client        :      1 :         49 :           3 :        0
  SSL/TLS/DTLS           :      1 :         49 :           3 :        0
Clientless VPN           :      0 :          1 :           1
  Browser                :      0 :          1 :           1
--------------------------------------------------------------------------------


   Total Active and Inactive    :      1            Total Cumulative :     50
   Device Total VPN Capacity    :  10000
   Device Load                  :     0%
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   Tunnels Summary
   --------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------
   Clientless                :      0 :          1 :               1
   AnyConnect-Parent         :      1 :         49 :               3
   SSL-Tunnel                :      1 :         46 :               3
   DTLS-Tunnel               :      1 :         46 :               3
   --------------------------------------------------------------------------------
   Totals                    :      3 :        142
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   IPv6 Usage Summary
   --------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------
   AnyConnect SSL/TLS/DTLS   :        :            :
     Tunneled IPv6           :      1 :         20 :           2
   --------------------------------------------------------------------------------
```

Step 5 Use the **show vpn-sessiondb anyconnect** command to view detailed information about current AnyConnect VPN sessions. Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN connection, you should see the bytes transmitted/received numbers change as you re-issue this command.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

View Remote Access VPN Configuration Details of FDM-Managed Device

Procedure

Step 1 In the left pane, click **VPN** > **Remote Access VPN Configuration**.

Step 2 Click on a VPN configuration object present.

The group shows summary information on how many connection profiles and group policies are currently configured.

- Expand the RA VPN configuration to view all connection profiles associated with them.
  - Click the add + button to add a new connection profile.
  - Click the view button ( ) to open a summary of the connection profile and connection instructions. Under **Actions**, you can click **Edit** to modify the changes.
- You can click one of the following options under **Actions** to perform additional tasks:
  - Click **Group Policies** to assign/add group policies.
  - Click a configuration object or connection profile that you no longer need and click **Remove** to delete.

Monitor Remote Access Virtual Private Network Sessions

Remote access Virtual Private Network provides secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connection and user session performance at a glance. Security Cloud Control remote access VPN monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users. You can also disconnect remote access VPN sessions as needed.

The Remote Access Virtual Private Monitoring page provides the following information:

- A list of active and historical sessions for up to a year.
- Shows intuitive graphical visuals to provide at-a-glance views from all active VPN headends managed by Security Cloud Control.
- The live session screen shows the most used operating system and VPN connection profile in the Security Cloud Control tenant. It also shows the average session duration and data uploaded and downloaded.
- Filtering capabilities to narrow your search based on criteria such as device type, device names, session length, and the amount of data transmitted and received.

Related Information:

- Monitor Live AnyConnect Remote Access VPN Sessions, on page 510
- Monitor Historical AnyConnect Remote Access VPN Sessions, on page 511
- Search and Filter Remote Access VPN Sessions

- Customize the Remote Access VPN Monitoring View
- Export Remote Access VPN Sessions to a CSV File
- Disconnect Remote Access VPN Sessions on FDM-Managed Device

Monitor Live AnyConnect Remote Access VPN Sessions

You can monitor real-time data from active AnyConnect remote access VPN sessions on the devices. This data is automatically refreshed every 10 minutes. If you want to retrieve the latest list of sessions at any point, you click the reload icon appearing on the right corner of the screen.

Before you begin

- Onboard the remote access VPN head-ends to Security Cloud Control.
- Ensure that the connectivity status of the devices you want to monitor live data is "Online" on the **Inventory** page.

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Remote Access Monitoring**.

Step 2 Click **RA VPN**.

Step 3 Click **Live**.

You can Search and Filter Remote Access VPN Sessions to narrow down your search based on criteria such as device type, session length, and upload and download data range.

Note The **Data TX** and **Data RX** information are not available for FTD.

View Live Remote Access VPN Data

The live data is presented both in the dashboard and tabular form.

Dashboard View

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard.

The dashboard provides at-a-glance views from all active VPN headends managed by Security Cloud Control.

- **Breakdown (All Devices)**: Shows a total number of live sessions. It also shows a pie chart that is divided into four arc lengths. It illustrates the percentage of VPN sessions of the top three devices with the highest number of sessions. The remaining arc length represents the aggregate of other devices.
- Shows most used operating system and connection profile in the Security Cloud Control tenant.
- Shows average session duration and data uploaded and downloaded.
- **Active Sessions by Country**: Shows an interactive heat map of the location of the users connected to your RA VPN headends.

- Countries from which users have connected are shown in progressively darker shades of blue, depending on the relative proportion of the sessions established from that country — the darker the blue color means more sessions are established from that country.
- The legend at the bottom of the map provides a scale that indicates the correlation between the number of sessions in a country and the shade of blue used to color the country.
- Hover the mouse pointer on the map to see the country's name and the total number of active user sessions established from that country.
- Hover the mouse pointer on the table to see the country's location and the total number of active user sessions on the map.

Tabular View

Click the **Show Tabular View** icon on the top right corner of the screen to view the data in tabular format.

The tabular form provides a complete list of VPN users connected presently.

- The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important Security Cloud Control applies a standard filter to the live data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the custom filters are not supported in the visual dashboard view. Click **Clear** to remove all filters you have applied. You cannot remove the standard filter.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Monitor Historical AnyConnect Remote Access VPN Sessions

You can monitor the historical data from AnyConnect Remote Access VPN sessions recorded over the last three months.

Before you begin

- Onboard the RA VPN head-ends to Security Cloud Control.

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Remote Access Monitoring**.

Step 2 Click **RA VPN**.

Step 3 Click **Historical**.

- Remote Access VPN Session data is stored and available to query for 1 year.
- You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range.
- The **Data TX** and **Data RX** information are not available for Secure Firewall Threat Defense.

View Historical Remote Access VPN Data

The historical data is presented both in the dashboard and tabular form.

Dashboard View

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard. You will see the dashboard view along with the tabular view.

The dashboard provides at-a-glance views from all active VPN headends managed by Security Cloud Control. It provides a bar graph showing the VPN sessions recorded for all devices in the last 24 hours, 7 days, and 30 days. You can select the duration from the drop-down. You can hover over on individual bars to see the date and the total number of sessions on that day.

Tabular View

You have to click the **Show Tabular View** icon appearing at the top right corner of the screen to see only the tabular view. The tabular form provides a complete list of VPN users connected over the last year.

The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important Security Cloud Control applies a standard filter to the historical data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the dashboard is not supported for custom filters. Clearing the newly applied filters relaunches the dashboard (On the screen, click **Clear** to remove manually applied filters). You cannot remove the standard filter.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as session date and time range, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Search and Filter Remote Access VPN Sessions

Search

Use the search bar functionality to find remote access VPN sessions. Start typing device name, IP address, or serial number in the search bar, and remote access VPN sessions that fit the search criteria will be displayed. Search is not case-sensitive.

Filter

Use the filter sidebar to find remote access VPN sessions based on criteria such as session time range, session length, and upload and download data range. The filter functionality is available to both live and historical views.

- **Filter by Devices**: Select one or all devices from the **All Types** tab to view sessions from selected devices. The window also categorizes the devices based on their type and displays them under the corresponding tabs.
- **Sessions Time Range** (Applicable only for historical data): View historical sessions from a specified date and time range. Note that you can view data recorded over the last three months.
- **Sessions Length**: View sessions based on a specified session's duration length. Set the time unit (hours, minutes, or seconds) and specify the minimum and maximum duration length by moving the slider. You can also specify the length in the provided fields.
- **Upload (TX)**: View sessions based on a specified amount of data uploaded or transferred to the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.
- **Download (RX)**: View sessions based on a specified amount of data downloaded or received from the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.

Customize the Remote Access VPN Monitoring View

You can modify the remote access VPN monitoring view in both live and historical modes to only include column headers that apply to the view you want. Click the column filter icon located to the right of the columns and select or deselect the columns you want.

Security Cloud Control remembers your selection the next time you sign in to Security Cloud Control.

Export Remote Access VPN Sessions to a CSV File

You can export the remote access VPN sessions of one or more devices to a comma-separated value (.csv) file. You can open the .csv file in a spreadsheet application such as Microsoft Excel to sort and filter the items on your list. This information helps you to analyze the remote access VPN sessions. Every time you export the sessions, Security Cloud Control creates a new .csv file, where the file created has a date and time in its name.

Security Cloud Control can export a maximum of 100,000 active sessions to the CSV file. If the total number of sessions from all devices exceeds the maximum limit, you can use the **View By Device** filter and generate reports for individual devices.

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Remote Access Monitoring**.

Step 2 In the **View By Devices** area, select one of the following:

- **All Devices** to export active sessions from all devices listed below it.
- Click on a device that you want to export sessions of that device.

Step 3 Click the icon on the top right corner. Security Cloud Control exports the rules you see on the screen to a .csv file.

Step 4 Open the .csv file in a spreadsheet application to sort and filter the results.

Remote Access VPN Dashboard

Security Cloud Control provides a consolidated information about remote access VPN connections from ASA, cloud-delivered Firewall Management Center-managed threat defense, and FDM-managed devices.

In the left pane, click **Secure Connections** > **Remote Access VPN**.

Disconnect Remote Access VPN Sessions on FDM-Managed Device

Currently, it is not possible to terminate remote access VPN sessions on an FDM-managed device using the Security Cloud Control interface. Instead, you can connect to the Threat Defense CLI using SSH and disconnect the desired user. You can perform this task on an online FDM-managed device onboarded to Security Cloud Control.

Procedure

Step 1 Log on to Firewall device manager and use the device CLI as explained in the **Logging Into the Command Line Interface (CLI)** section of the "Getting Started" chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Step 2 Execute the `vpn-sessionsdb logoff {name}` command and replace **name** with the user name. This command terminates all sessions for the username that you specify.

Templates

Templates provide the means to develop a preferred and general use version of device configuration files:

- Templates are created from an existing base configuration file.
- They support value parameters for easy customization of expected values, including IP addresses and port numbers.
- They are exportable, with parameter substitution, for use across multiple devices.

Related Information

- FDM-Managed Device Templates, on page 515
  - Configure an FDM Template, on page 516
  - Apply Template to an FDM-Managed Device, on page 520

FDM-Managed Device Templates

About FDM-Managed Device Templates

Security Cloud Control allows you to create a FDM-managed device template of an onboarded FDM-managed device's configuration. When you are creating the template, select the parts (objects, policies, settings, interfaces, and NAT) that you want to include in your FDM-managed device template. You can then modify that template and use it to configure other FDM-managed devices you manage. FDM-managed device templates are a way to promote policy consistency between your FDM-managed devices.

When creating the FDM-managed device template, you can opt to either create a complete or custom template:

- A complete template includes all parts of the FDM-managed device configuration and applies everything on other FDM-managed devices.
- A custom template includes only one or more parts of the FDM-managed device configuration that you select and applies only that part and its associated entities on other FDM-managed devices.

Important The FDM-managed device template will not include certificate, Radius, AD, and RA VPN Objects.

How You Could Use FDM-Managed Device Templates

Here are some ways that you could use FDM-managed device templates:

- Configure one FDM-managed device by applying another FDM-managed device's configuration template to it. The template you apply may represent a "best practice" configuration that you want to use on all your FDM-managed devices.
- Use the template as a method to make the device configuration changes and simulate them in a lab environment to test its functionality before applying those changes to a live FDM-managed device.
- Parameterize the attributes of the interfaces and sub-interfaces when creating a template. You can change the parameterized values of interfaces and subinterfaces at the time of applying the template.

What You Will See in the Change Log

When you apply a template to a device, you overwrite the entire configuration of that device. The Security Cloud Control change log records every change that gets made as a result. So, change log entries will be very long after applying a template to a device.

Related Information:

- Configure an FDM Template
- Apply an FDM Template

Configure an FDM Template

Prerequisites

Before you create a FDM-managed device template, onboard to Security Cloud Control the FDM-managed device from which you will create the template. You can only create an FDM-managed device template from an onboarded FDM-managed device.

We **strongly** recommend using templates to configure brand new FDM-managed devices being added to your environment.

Note When you create a template from an FDM-managed device, the RA VPN objects are not included in the template.

Create an FDM Template

When creating a template, if you select all parts, the template will include every aspect of that device's configuration; it's management IP address, interface configurations, policy information, and so on.

If you select some of the parts, the custom template includes the following entities.

Template Parts	Parts included in Custom Template
Access Rules	Includes access control rules and any related entities for those rules. For example, objects and interfaces (with sub-interfaces).
NAT Rules	Includes NAT rules and any related entities required for those NAT rules. For example, objects and interfaces (with sub-interfaces).
Settings	Includes system settings and any related entities required for those settings. For example, objects and interfaces (with sub-interfaces).
Interfaces	Includes interfaces and sub-interfaces.
Objects	Includes objects and any related entities required for those objects. For example, interfaces and sub-interfaces.

Use this procedure to create an FDM-managed device template:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 Use the Filters or Page Level Search field to find the FDM-managed device from which you want to create the template.

Step 5 In the **Device Actions** pane on the right, click **Create Template**. The **Name Template** provides the count of each part on the device. It also shows the count of sub-interfaces, if any.

Step 6 Select the parts that you want to include in the template.

Step 7 Enter a name for your template.

Step 8 Click **Create Template**.

Step 9 In the **Parameterize Template** area, you can perform the following:

- To parameterize an interface, hover (until you see curly braces) and click a cell corresponding to that interface.
- To parameterize a sub-interface, expand the interface that has a sub-interface, and hover (until you see curly braces) and click a cell corresponding to that sub-interface.

You can parameterize the following attributes to enable per-device customization.

- **Logical Name**
- **State**
- **IP Address/Netmask**

Note These attributes only support one value per parameter.

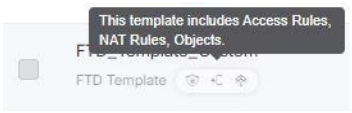
Step 10 Click **Continue**.

Step 11 Review the template and any parameterizations. Click **Done** to create the template.

The **Inventory** page now displays the FDM-managed device template you just created.

Note After creating a template, in the **Inventory** pane, Security Cloud Control displays the corresponding template part icons to show the parts included in that template. This information also appears in the **Device Details** pane when you click the device or when you hover over the mouse pointer on the icon.

The following picture shows an example of a part icon to show that the template includes "access rules", "NAT rules", and "objects".



Edit an FDM-Managed Device Template

Edit the template parameters with the following procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Templates** tab.

Step 3 Click the **FTD** tab.

Step 4 Use the Model/Template filter to find the template you want to modify.

Step 5 In the **Device Actions** pane on the right, click **Edit Parameters**.

Step 6 (Optional) make any changes to the parameters by directly editing the text box.

Step 7 Click **Save**.

You can edit the rest of the FDM-managed device template just as you would the configuration of a live FDM-managed device. You can edit your FDM-managed device template with the following configurations:

- FDM-Managed Device Settings
- Manage Virtual Private Network Management in Security Cloud Control
- Create an RA VPN Configuration
- FDM Policy Configuration
- Promote policy and configuration consistency

Delete an FDM Template

You delete an FDM-managed device template just as you would remove an FDM-managed device from Security Cloud Control:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Templates** tab.

Step 3 Click the **FTD** tab.

Step 4 Use the filter and search fields to find the FDM-managed device template you want to delete.

Step 5 In the **Device Actions** pane, click **Remove** .

Step 6 Read the warning message and click **OK** to delete the template.

Related Information:

- FDM-Managed Device Templates
- Apply an FDM Template

Apply an FDM Template

Before applying a template, you can identify its contents by navigating to the **Inventory** page and filter for **Model/Template**. Security Cloud Control displays the corresponding template part icons to show the parts included in that template. This information also appears in the **Device Details** pane when you click the device or when you hover over the mouse pointer on the icon.

You can parameterize the following attributes to enable per-device customization, which means you can apply device-specific values at the time of applying the template:

When applying the FDM-managed device template, you can change the parameterized values of interfaces and subinterfaces configured when creating the template.

Apply a Complete Template

Applying a complete FDM-managed device template to create a new FDM-managed device overwrites entirely any existing configuration on the FDM-managed device, including any staged changes that have not yet been deployed from Security Cloud Control to the device. Anything on the device that was not included in the template will be lost.

Apply a Custom Template

Applying a custom FDM-managed device template to other FDM-managed devices will retain or remove the existing configuration based on the template part. The following table provides the changes that occur after applying the custom template on other FDM-managed devices.

Template Parts	After Applying Custom Template
Access Rules	• New access control rules present in the custom template overwrites any existing access control rules on the device. • New objects and interfaces (with sub-interfaces), if any, in the custom template are applied to the device without deleting any existing objects and interfaces.
NAT Rules	• New NAT rules present in the custom template overwrites any existing NAT rules on the device. • New objects and interfaces (with sub-interfaces), if any, in the custom template are applied to the device without deleting any existing objects and interfaces.
Settings	• New system settings from the custom template are applied to the device without deleting any existing system settings. • New objects and interfaces (with sub-interfaces), if any, in the custom template are applied to the device without deleting any existing objects and interfaces.
Interfaces	• New interfaces and sub-interfaces from the custom template are applied to the device without deleting any existing interfaces and sub-interfaces. • Security Cloud Control does not allow applying a template to a device where more interfaces are defined in the template than there are interfaces on the device.
Objects	• New objects from the custom template are applied to the device without deleting any existing objects. • New interfaces and sub-interfaces, if any, in the custom template are applied to the device without deleting any existing interfaces and sub-interfaces.

Prerequisites

The following conditions must be met prior to applying a template:

- When using a template, be sure that any changes you have made to the template have been committed and that the template is in the "Synced" state on the **Inventory** page.
- When using an FDM-managed device as a template, be sure that any changes on Security Cloud Control you intended to deploy to the device have been deployed and that there are no changes from the firewall device manager console that have not been deployed. The device must show a Synced state on the **Inventory** page.

Applying the template to a device is a three-step process.

1. Apply a Complete Template
2. Review Device and Networking Settings
3. Deploy Changes to the Device

Apply Template to an FDM-Managed Device

Important Before you deploy the changes to the device, continue to the next procedure:

Review Device and Networking Settings

You can use Change Request Management to apply a tracking label to your changes before you apply the template. Use the following procedure to apply an FDM-managed device template:

Procedure

Step 1 (Optional) Before you begin, make a template of your FDM-managed device before you apply another template to it. This gives you a configuration backup you can reference when you need to reapply device and networking settings.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Templates** tab.

Step 4 Click the **FTD** tab.

Step 5 Use the filter and search field to find the FDM-managed device or template to which you are going to apply the template.

Note If you change the name of the template at this point, you are applying a full device configuration or template to *DeviceName*. Deploying this change to *DeviceName* will overwrite the entire configuration running on that device.

Step 6 In the device **Actions** pane on the right, click **Apply Template**.

Step 7 Click **Select Template** and select the desired template and click **Continue**.

Step 8 You can configure the following and click **Continue** appearing on each screen.

a. **Map Interfaces**: Confirm or change the mapping of interfaces between the template and the device. Note that you cannot have more than one template interface mapped to a single device interface; if the interface configuration is not supported, you cannot continue and apply the template.

Note Security Cloud Control does not allow applying a template to a device where more interfaces are defined in the template than there are interfaces on the device.

b. **Fill Parameters**: Customize the interface or sub-interface parameter values for the device that you are applying the template to.

c. **Review**: Review the template configuration and click **Apply Template** when you are ready to overwrite the existing device configuration with the configuration in the template.

Step 9 Click Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Review Device and Networking Settings

When creating an FDM-managed device template, Security Cloud Control copies the entire device configuration into the template. So, things like the management IP address of the original device are contained in the template. Review these device and network settings before you apply the template to a device:

Procedure

Step 1 Review these FDM-managed device settings to ensure that they reflect the correct information for the new FDM-managed device:

- FDM-Managed Device Settings
- Management Interface
- Hostname

Step 2 Review the Configure the FDM Access Control Policy to ensure that rules reference the new FDM-managed device's IP addresses where appropriate.

Step 3 Review inside_zone and outside_zone security objects to ensure they reference the correct IP address for the new FDM-managed device.

Step 4 Review NAT policies to ensure they reference the correct IP addresses for the new FDM-managed device.

Step 5 Review Interface configurations to ensure that they reflect the correct configuration for the new FDM-managed device.

Deploy Changes to the Device

Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- FDM-Managed Device Templates
- Configure an FDM Template

Migrating an ASA Configuration to an FDM-Managed Device Template

Attention Secure Firewall device manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. Open a Support Ticket with TAC to enable this platform.

Security Cloud Control helps you migrate your ASA to an FDM-managed device. Security Cloud Control provides a wizard to help you migrate these elements of the ASA's running configuration to an FDM-managed device template:

- Access Control Rules (ACLs)
- Interfaces
- Network Address Translation (NAT) rules
- Network objects and network group objects
- Routes
- Service objects and service group objects
- Site-to-site VPN

Once these elements of the ASA running configuration have been migrated to an FDM-managed device template, you can then apply the FDM template to a new FDM-managed device that is managed by Security Cloud Control. The FDM-managed device adopts the configurations defined in the template, and so, the FDM-managed device is now configured with some aspects of the ASA's running configuration.

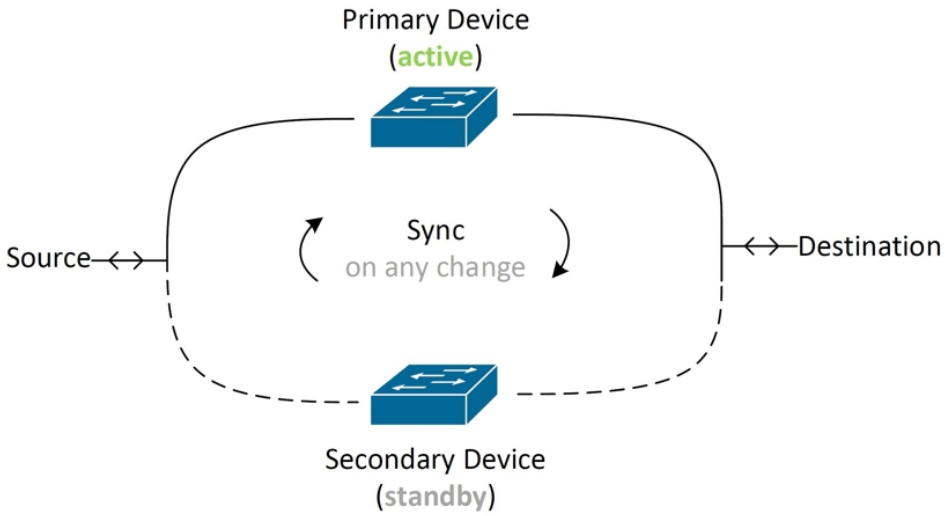
Other elements of the ASA running configuration are not migrated using this process. Those other elements are represented in the FDM-managed device template by empty values. When the template is applied to an FDM-managed device, we apply values we migrated to the new FDM-managed device and ignore the empty values. Whatever other default values the new FDM-managed device has, it retains. Those other elements of the ASA running configuration that we did not migrate, will need to be recreated on the FDM-managed device outside the migration process.

See Migrating an ASA to an FDM-Managed Device Using Cisco Security Cloud Control for a full explanation of the process of migrating an ASA to an FDM-managed device using Security Cloud Control.

FDM-Managed High Availability

About High Availability

A high availability (HA), or failover configuration, joins two devices into a primary/secondary setup so that if the primary device fails, the secondary automatically takes over. Configuring high availability, also called failover, requires two identical FDM-managed devices connected to each other through a dedicated failover link and, optionally, a state link. The health of the active unit (hardware, interfaces, software, and environmental status) is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs. This helps keep your network operation in case of a device failure or during a maintenance period when the devices are upgrading. See the related articles below for more information.



The units form an active/standby pair, where the primary unit is the active unit and passes traffic. The secondary (standby) unit does not actively pass traffic, but synchronizes configuration and other state information from the active unit. The two units communicate over the failover link to determine the operating status of each unit.

Note When you opt to accept changes from or deploy to an FDM-managed HA pair, you are communicating with the active device of the HA pair. This means that configurations and backups are pulled from the active device only.

Certificate and High Availability Pairs

When you apply a certificate to an FDM-managed HA pair, Security Cloud Control only applies the certificate to the active device; only upon deploying the active device is the configuration, and the certificate, synchronized with the standby device. If you apply a new certificate to the active device through FDM-managed, the active device and standby device may have two different certificates. This may cause issues in failover or failover history, among other possible issues. The two devices must have the same certificate to function successfully. If you must change the certificate through FDM-managed, then you must deploy changes and synchronize the certificate within the HA pair.

Related Information:

- Failover and Stateful Link for FDM-Managed High Availability
- FDM-Managed High Availability Pair Requirements
- Create an FDM-Managed High Availability Pair
- FDM-Managed Devices in High Availability Page
- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History

- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair
- Upgrade an FDM-Managed High Availability Pair
- About Device Configuration Changes
- Read Configuration Changes from FDM-Managed Device to Security Cloud Control
- Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device

FDM-Managed High Availability Pair Requirements

High Availability Requirements

There are several requirements you must establish before you create a high availability (HA) pair.

Physical and Virtual Device Requirements for HA

The following hardware requirements must be met:

- The devices must be the same hardware model.
- The devices must have the same modules installed. For example, if one has an optional network module, then you must install the same network module in the other device.
- The devices must have the same type and number of interfaces.
- To create an HA pair in Security Cloud Control, both devices must have management interfaces configured. If the devices have data interfaces configured, you must create the HA pair through the FDM-managed UI, and then onboard the pair to Security Cloud Control.

Note You **cannot** use an FDM-managed template in an HA pair.

Software Requirements for HA

The following software requirements must be met for both physical and virtual FDM-managed devices:

- You have two standalone FDM-managed devices onboarded in the Security Cloud Control.
- The devices must run the exact same software version, which means the same major (first), minor (second), and maintenance (third) numbers. You can find the version inside the Device Details window on the **Inventory** page, or you can use the show version command in the CLI.

Note Devices with different versions are allowed to join, but the configuration is not imported into the standby unit and failover is not functional until you upgrade the units to the same software version.

- Both devices must be in local manager mode, that is, configured using FDM. If you can log into FDM on both devices, they are in local manager mode. You can also use the show managers command in the CLI to verify.
- You must complete the initial setup wizard for each device before onboarding to Security Cloud Control.
- Each device must have its own management IP address. The configuration for the management interface is not synchronized between the devices.
- The devices must have the same NTP configuration.
- You cannot configure any interface to obtain its address using DHCP. That is, all interfaces must have static IP addresses.

  Note: If you change any interface configurations, you must deploy the changes to the device before establishing HA.
- Both devices must be **synced**. If you have pending changes or conflicts detected, see Resolve Configuration Conflicts and Resolve Configuration Conflicts for more information.

Note When you opt to accept changes from or deploy to an FDM-managed HA pair, you are communicating with the active device of the HA pair. This means that configurations and backups are pulled from the active device only.

Smart License Requirements for HA

The following license requirements must be met for both physical and virtual FDM-managed devices:

- Both devices in an HA pair must have either a registered license, or an evaluation license. If the devices are registered, they can be registered to different Cisco Smart Software Manager accounts, but the accounts must have the same state for the export-controlled functionality setting, either both enabled or both disabled. However, it does not matter if you have enabled different optional licenses on the devices.
- Both devices within the HA pair must have the same licenses during operation. It is possible to be in compliance on one device, but out of compliance on the other if there are insufficient licenses. If your Smart Licenses account does not include enough purchased entitlements, your account becomes Out-of-Compliance (even though one of the devices may be compliant) until you purchase the correct number of licenses.

Note that if the device is in evaluation mode, you must ensure that the registration status for Security Cloud Control is the same on the devices. You must also ensure that your selection for participation in the Cisco Success Network is the same. For registered devices, the settings can be different on the units, but whatever is configured on the primary (active) device will either register or unregister the secondary. An agreement to participate in the Cisco Success Network on the primary implies an agreement for the secondary.

If you register the devices to accounts that have different settings for export controlled features, or try to create an HA pair with one unit registered and the other in evaluation mode, the HA join might fail. If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. This will impact routing on the supported network segments, and you will have to manually break HA on the secondary unit to recover.

Cloud Services Configuration for HA

Both of the devices within an HA pair must have **Send Events to the Cisco Cloud** enabled. This feature is available in the FDM UI. Navigate to **System Settings** and click **Cloud Services** to enable this feature. Without this option enabled, the HA pair cannot form in Security Cloud Control and an event description error occurs. See the **Configuring Cloud Services** chapter of the Firepower Device Manager Configuration Guide of the version you are running for more information.

Create an FDM-Managed High Availability Pair

Before you create an FDM-managed HA pair in Security Cloud Control, you must first onboard two standalone FDM-managed devices that meet the requirements described in FDM-Managed High Availability Pair Requirements.

Note To create an HA pair in Security Cloud Control, both devices must have management interfaces configured. If the devices have data interfaces configure, you must create the HA pair through the FDM console, and then onboard the pair to Security Cloud Control.

Once you create an FDM-managed HA pair, the primary device is **active** and the secondary device is **standby** by default. All configuration changes or deployments are made through the primary device and the secondary device remains in standby mode until the primary unit becomes unavailable.

Note that when you opt to accept configuration changes from or deploy to an FDM-managed HA pair, you are communicating with the active device of the HA pair. Any changes made to the primary device are transferred over the link between the primary and the secondary device. Security Cloud Control deploys to and accepts changes only from the primary device; thusly, the **Inventory** page displays a single entry for the pair. Once the deploy occurs, the primary device synchronized any configuration changes to the secondary device.

Simi liar to how Security Cloud Control communicates with only the active device, when you schedule or opt to back up an FDM-managed HA pair, only the active device is eligible to back up.

Note If the HA devices experience an issue during the creation process or the HA pair does not result with a healthy status, you must manually break the HA configuration before you attempt to create the pair again.

Procedure

Create an HA pair from two standalone FDM-managed devices with the following procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD**tab and select the device you want to establish as the primary device.

Note Security Cloud Control does not support creating an HA pair with devices configured with DHCP.

Step 4 In the Management pane, click **High Availability**.

Step 5 Locate the area for the secondary device and click **Select Device**, then choose a device from the list of eligible devices.

Step 6 Configure the Failover link.

a. Click **Physical Interface**and select an interface from the drop-down menu.

b. Select the appropriate **IP Type**.

c. Enter the **Primary IP** address.

d. Enter the **Secondary IP** address.

e. Enter the **Netmask**. By default, this value is 24.

f. If applicable, enter a valid **IPSec Encryption Key**.

Step 7 Configure the Stateful link. If you want to use the same configuration as the failover link, check the **The same as Failover Link** checkbox. If you want to use a different configuration, use the following procedure:

a. Click **Physical Interface** and select an interface from the drop-down menu. Note that both the primary and secondary device **must** have the same number of physical interfaces.

b. Select the appropriate **IP Type**.

c. Enter the **Primary IP** address.

d. Enter the **Secondary IP** address.

e. Enter the **Netmask**. By default, this value is 24.

Step 8 Click **Create** in the upper right corner of the screen to finish the wizard. Security Cloud Control immediately redirects you to the High Availability Status page. From this page you can monitor the status of the HA creation. Note that once the HA pair is created, the **Inventory** page displays the pair as a single row.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

FDM-Managed Devices in High Availability Page

The FDM-managed in High Availability (HA) management page is a multi-purpose page for FDM-managed devices. This page is only available for devices that are already configured as an HA pair. You can onboard an FDM-managed HA pair or you can create an FDM-managed HA pair from two standalone FDM-managed devices.

If you select a standalone FDM-managed device from the **Inventory** page, this page acts as a wizard for creating an HA pair. At this time, you must have two FDM-managed devices onboarded to Security Cloud Control to create a pair. To create an FDM-managed HA pair in Security Cloud Control, see Create an FDM-Managed High Availability Pair.

If you select an FDM-managed HA pair from the **Inventory** page, this page acts as an overview page. From here you can view the HA configuration and the failover history, as well as actionable items such as force a failover, edit the failover criteria, and remove the HA link.

High Availability Management Page

To see the High Availability page, use the following procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select a standlalone FDM-managed device **or** the active FDM-managed device of the FDM-managed HA pair.

Step 4 In the **Management** pane, click **High Availability**.

Related Information:

- FDM-Managed High Availability Failover History
- Edit High Availability Failover Criteria
- Force a Failover on an FDM-Managed High Availability Pair
- Break an FDM-Managed High Availability Pairing
- Refresh the FDM-Managed High Availability Status

Edit High Availability Failover Criteria

You can edit the failover criteria after the FDM-managed HA pair is created.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select the active device of the FDM-managed HA pair.

Step 4 In the **Management** pane, click **High Availability**.

Step 5 In the Failover Criteria window click **Edit**.

Step 6 Make any necessary changes and click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes now you made to the active device, or wait and deploy multiple changes at once.

Break an FDM-Managed High Availability Pairing

When you break HA, the configured interfaces on the standby device are automatically disabled. The devices may experience a disruption in traffic during this process. After the HA pair is successfully removed you will be redirected from the status page to the High Availability page where you will have the option to create another HA pair with the same primary device.

Note You cannot deploy to either of the devices until the HA pair is successfully removed.

Break HA with Management Interfaces

When you break HA for a pair that is configure with management interfaces, the break may take 10 minutes or longer to complete and both devices go offline during this process. When the HA configuration is successfully removed, Security Cloud Control displays both units as standalone devices in the **Services & Devices** page.

Break HA with Data Interfaces

When you break HA for a pair that is configured with data interfaces, the break may take 20 minutes or more to complete and both of the devices go offline. you must manually reconnect the active device after the HA configuration is removed.

The standby device retains the HA configuration, though, and will become unreachable since it has the same configuration as the active device. You must manually reconfigure the IP interfaces outside of Security Cloud Control, and then re-onboard the device as a standalone.

Break High Availability

Use the following procedure to remove the HA pairing of two FDM-managed devices:

Procedure

Step 1 In the navigation bar, click **Security Devices** and select the active device of the FDM-managed HA pair.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 In the Management pane, click **High Availability**.

Step 5 Click **Break High Availability**.

Step 6 Security Cloud Control removes the HA configuration and both devices are displayed as standalone devices in the **Inventory** page.

Step 7 Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device to deploy the new configuration to both devices.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made to the active device now, or wait and deploy multiple changes at once.

Break Out-of-Band High Availability

If you break an FDM-managed HA pair using the FDM interface, the configuration status of the HA pair in Security Cloud Control changes to **Conflict Detected.** After you break HA, you must deploy the changes to the primary device through FDM-managed and then Resolve Configuration Conflicts state in Security Cloud Control.

After the device is back in the Synced state, you can deploy configuration changes made in Security Cloud Control to the device.

We do **not** recommend reverting changes from Security Cloud Control after breaking HA using the FDM-managed interface.

Related Information:

- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair
- About Device Configuration Changes

Force a Failover on an FDM-Managed High Availability Pair

Switch the active and standby devices within an FDM-managed HA pair by forcing a failover. Note that if you recently applied a new certificate to the active device and have **not** deployed changes, the standby device retains the original certificate and failover will fail. The active and standby devices must have the same certificate applied. Use the following procedure to manually force a failover:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select the active device of the FDM-managed HA pair.

Step 5 In the Management pane, click **High Availability**.

Step 6 Click the options icon .

Step 7 Click **Switch Mode**. The active device is now on standby, and the standby device is now active.

Related Information:

- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair

FDM-Managed High Availability Failover History

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select the active device of the FDM-managed HA pair.

Step 5 In the Management pane, click **High Availability**.

Step 6 Click **Failover History**. Security Cloud Control generates a window that details the failover history for both the primary and secondary device since the HA pair was formed.

Note Failover history is also displayed in the pair's change log, available from the **Inventory** page.

Related Information:

- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair

Refresh the FDM-Managed High Availability Status

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select the FDM-managed device or the FDM-managed HA pair.

Step 4 In the **Management** pane, click **High Availability**.

Step 5 Click the options icon  .

Step 6 Click **Get Latest Status**. Security Cloud Control requests a health status from the primary device.

Related Information:

- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair

Failover and Stateful Link for FDM-Managed High Availability

Failover Link and (Optional) Stateful Link

The failover link is a dedicated connection between the two units. The stateful failover link is also a dedicated connection, but you can either use the one failover link as a combined failover/state link, or you can create a separate, dedicated state link. If you use just the failover link, the stateful information also goes over that link: you do not lose stateful failover capability. By default, the communications on the failover and stateful failover links are plain text (unencrypted). You can encrypt the communications for enhanced security by configuring an IPsec encryption key.

You can use any unused data physical interfaces as the failover link and optional dedicated state link. However, you cannot select an interface that is currently configured with a name, or one that has subinterfaces. The failover and stateful failover link interfaces are not configured as normal networking interfaces. They exist for failover communication only, and you cannot use them for through traffic or management access. Because the configuration is synchronized between the devices, you must select the same port number for each end of a link. For example, GigabitEthernet1/3 on both devices for the failover link.

Note The FDM-managed device does not support sharing interfaces between user data and the failover link.

Failover Link

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit and to synchronize configuration changes. The following information is shared over the link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

You can use an unused data interface (physical, redundant, or EtherChannel) as the failover link; however, you cannot specify an interface that is currently configured with a name. Do **not** use a subinterface as the failover link.

The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface can only be used for the failover link (and also for the state link).

Stateful Link

The active unit uses the state link to pass connection state information to the standby device. This means that the standby unit can maintain certain types of connections without impacting the user. This information helps the standby unit maintain existing connections when a failover occurs.

You can use a dedicated data interface (physical, redundant, or EtherChannel) for the state link. For an EtherChannel used as the state link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used.

Using a single link for both the failover and stateful failover links is the best way to conserve interfaces. However, you must consider a dedicated interface for the state link and failover link, if you have a large configuration and a high traffic network. We recommend that the bandwidth of the stateful failover link should match the largest bandwidth of the data interfaces on the device.

FDM-Managed Device Settings

Configure an FDM-Managed Device's System Settings

Use this procedure to configure settings on a single FDM-managed device:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select the FDM-managed device you want to configure the settings. To narrow down your search results and easily find the FDM-managed devices, you can make use of the filter button.

Step 4 In the **Management** pane at the right, click **Settings**.

Step 5 Click the **System Settings** tab.

Step 6 Edit any of these device settings:

- Configure Management Access
- Configure Logging Settings
- Configure DHCP Servers
- Configure DNS Server
- Hostname
- Configure NTP Server
- Configure URL Filtering
- Cloud Services
- Enabling or Disabling Web Analytics

Configure Management Access

By default, you can reach the device's management address from any IP address. System access is protected by username and password only. However, you can configure an access list to allow connections from specific IP addresses or subnets only to provide another level of protection.

You can also open data interfaces to allow an FDM-managed device or SSH connections to the CLI. You can then manage the device without using the management address. For example, you could allow management access to the outside interface, so that you can configure the device remotely. The username and password protects against unwanted connections. By default, HTTPS management access to data interfaces is enabled on the inside interface, but it's disabled on the outside interface. For device models that have a default "inside" bridge group, this means that you can make FDM-managed device connections through any data interface within the bridge group to the bridge group IP address (default is 192.168.1.1). You can open a management connection only on the interface through which you enter the device.

Caution If you constrain access to specific addresses, you can easily lock yourself out of the system. If you delete access for the IP address that you are currently using, and there's no entry for "any" address, you'll lose access to the system when you deploy the policy. Be mindful of this when configuring the access list.

Create Rules for Management Interfaces

Use the following procedure to create rules for managment interfaces:

Procedure

Step 1 Click **New Access** in the Management Interface section.

- **Protocol**. Select whether the rule is for HTTPS (port 443) or SSH (port 22).
- **Allowed Networks**. Select the network object that defines the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6**(::/0).

Step 2 Click **Save**.

Create Rules for Data Interfaces

Use the following procedure to create rules for data interfaces:

Procedure

Step 1 Click **New Access** in the Data Interface section.

- **Interface**. Select the interface on which you want to allow management access.
- **Protocol**. Select whether the rule is for HTTPS (port 443), SSH (port 22), or both. You cannot configure HTTPS rules for the outside interface if it's used in a remote access VPN connection profile.
- **Allowed Networks**. Select the network object that defines the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6** (::/0).

Step 2 Click **Save**.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure Logging Settings

This procedure describes how to enable logging of diagnostic (data) messages, file and malware events, intrusion events, and console events. Connection events are not logged as a result of these settings; they are logged if connection logging is configured on access rules, security intelligence policies, or SSL decryption rules.

Procedure

Step 1 Configure an FDM-Managed Device's System Settings.

Step 2 On the System Settings page click **Logging** in the settings menu.

Step 3 **Data logging**. Slide the **Data Logging** slider to **On** to capture diagnostic logging syslog messages. Click the plus button  to specify the Syslog Server Objectsthat represents the syslog server that you want to send the events to. (You can also create a syslog server object at this point.) Additionally, select the minimum level of Message Severity Levels you want to log.

This will send data logging events for any type of syslog message, with your minimum chosen severity level, to the syslog server.

Note Security Cloud Control doesn't currently support creating a Custom Logging Filter for Data Logging. For finer control of which messages you send to the syslog server, we recommend you define this setting in an FDM-managed device. To do so, log on to an FDM-managed device, and navigate **System Settings** > **Logging Settings**.

Tip Do not enable data logging if you are a Cisco Security Analytics and Logging customer *unless* you forward the data logging events to a syslog server other than the Secure Event Connectors. Data events (diagnostic events) are not traffic events. Sending the data events to a different syslog server removes the burden on the SEC from analyzing and filtering them out.

Step 4 **File/Malware Log Settings**. Slide the slider to **On** to capture file and malware events. Specify the Syslog Server Objects that represents the syslog server that you want to send the events to. You can also create a syslog server object at this point if you have not already.

File and malware events are generated at the same severity level. The minimum level of Message Severity Levels you select will be assigned to all file and malware events.

File and malware events are reported when a file or malware policy in any access control rule has been triggered. This is not the same as a connection event. Note that the syslog settings for file and malware events are relevant only if you apply file or malware policies, which require the and Malware licenses.

For Cisco Security Analytics and Logging subscribers:

- If you send events to the Cisco cloud through a Secure Event Connector (SEC), specify an SEC as your syslog server. You will then be able to see these events alongside file policy and malware policy connection events.

- If you send events directly to the Cisco cloud without an SEC, you do not need to enable this setting. File and malware events are sent if the access control rule is configured to send connection events.

Step 5 **Intrusion Logging**. Send intrusion events to a syslog server by specifying the Syslog Server Objects that represents the syslog server you want to send events to. You can also create a syslog server object at this point if you have not already.

Intrusion events are reported when an intrusion policy in any access control rule has been triggered. This is not the same as a connection event. Note that the syslog settings for intrusion events are relevant only if you apply intrusion policies, which require the license.

For Cisco Security Analytics and Logging subscribers:

- If you send events to the Cisco cloud through a Secure Event Connector (SEC), specify an SEC as your syslog server. You will then be able to see these events alongside file policy and malware policy connection events.
- If you send events directly to the Cisco cloud without an SEC, you do not need to enable this setting. Intrusion events are sent to the Cisco cloud if the access control rule is configured to send connection events.

Step 6 **Console Filter**. Slide the slider to **On** to send data logging (diagnostic logging) events to a console rather than to a syslog server. Additionally, select the minimum level of event severity you want to log. This will send a data logging event for any type of syslog message, with your chosen severity level.

You will see these messages when you log into the CLI on the console port of your FDM-managed device. You can also see these logs in an SSH session to other FDM-managed device interfaces (including the management interface) by using the **show console-output** command. In addition, you can see these messages in real time in the diagnostic CLI by entering **system support diagnostic-cli** from the main CLI.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Message Severity Levels

The following table lists the syslog message severity levels.

Level Number	Severity Level	Description
0	**emergencies**	System is unusable.
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.

Level Number	Severity Level	Description
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only.
Note	FDM-managed device does not generate syslog messages with a severity level of zero (emergencies).	

Configure DHCP Servers

A Dynamic Host Configuration Protocol (DHCP) server provides network configuration parameters, such as IP addresses, to DHCP clients. You can configure a DHCP server on an interface to provide configuration parameters to DHCP clients on the attached network.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68. The DHCP server listens for messages on UDP port 67. The DHCP server does not support BOOTP requests.

DHCP clients must be on the same network as the interface on which the server is enabled. There cannot be an intervening router between the server and client, although there can be a switch.

Caution Do not configure a DHCP server on a network that already has a DHCP server operating on it. The two servers will conflict with each other, and the results will be unpredictable.

Procedure

Step 1 The section has two areas. Initially, the Configuration section shows the global parameters. The DHCP Servers area shows the interfaces on which you have configured a server, whether the server is enabled, and the address pool for the server.

Step 2 In the **Configuration** section, configure auto configuration and global settings.

DHCP auto configuration enables the DHCP server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that's running on the specified interface. Typically, you would use auto configuration if you're obtaining an address using DHCP on the outside interface, but you could choose any interface that obtains its address through DHCP. If you cannot use auto configuration, you can manually define the required options.

a. Click the **Enable Auto Configuration** slider to On if you want to use auto configuration, and in the **From Interface** pull-down, select the interface that's obtaining its address through DHCP.

b. If you do not enable auto configuration, or if you want to override any of the automatically configured settings, configure the following global options. These settings are sent to DHCP clients on all interfaces that host DHCP server.

1. **Primary WINS IP Address**, **Secondary WINS IP Address**. The addresses of the Windows Internet Name Service (WINS) servers that clients should use for NetBIOS name resolution.

2. **Primary DNS IP Address**, **Secondary DNS IP Address**. The addresses of the Domain Name System (DNS) servers that clients should use for domain name resolution. Click **Apply Umbrella Settings** if you want to populate the DNS IP address fields with Cisco Umbrella DNS servers. Clicking the button loads the appropriate IP addresses into the fields.

c. Click **Save**.

Step 3 In the DHCP Servers section, either edit an existing server, or click **New DHCP Server** to add and configure a new server.

a. Configure the server properties:

1. **Enable DHCP Server**. Whether to enable the server. You can configure a server but keep it disabled until you are ready to use it.
2. **Interface**. Select the interface on which you will provide DHCP addresses to clients. The interface must have a static IP address; you cannot be using DHCP to obtain the interface address if you want to run a DHCP server on the interface. For bridge groups, you configure the DHCP server on the Bridge Virtual Interface (BVI), not the member interfaces, and the server operates on all member interfaces. You cannot configure DHCP server on the Diagnostic interface, configure it on the Management interface instead, on the **Device** > **System Settings > Management Interface** page.
3. **Address Pool**. Add the single IP address or an IP address range of a DHCP server. The range of IP addresses from lowest to highest that the server is allowed to provide to clients that request an address. The range of IP addresses must be on the same subnet as the selected interface and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address. Specify the start and end address for the pool, separated by a hyphen. For example, 10.100.10.12-10.100.10.250.

b. Click **OK**.

Step 4 Click **Save**.

Step 5 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure DNS Server

A Domain Name System (DNS) server is used to resolve hostnames to IP addresses. DNS servers are used by the management interface.

Procedure

Step 1 In **Primary, Secondary, Tertiary DNS IP Address**, enter the IP addresses of up to three DNS servers in order of preference. The primary DNS server is used unless it cannot be contacted, in which case the secondary is tried, and finally the tertiary. Click **Apply Umbrella Settings** if you want to populate the DNS IP address fields with Cisco Umbrella DNS servers. Clicking the button loads the appropriate IP addresses into the fields.

Step 2 In **Domain Search Name**, enter the domain name for your network; for example, example.com. This domain gets appended to hostnames that are not fully qualified; for example, serverA becomes serverA.example.com.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Management Interface

The management interface is a virtual interface attached to the physical management port. The physical port is named the Diagnostic interface, which you can configure on the Interfaces page with the other physical ports. On virtual FDM-managed devices, this duality is maintained even though both interfaces are virtual.

The management interface has two uses:

- You can open web and SSH connections to the IP address and configure the device through the interface.
- The system obtains smart licensing and database updates through this IP address.

If you use the CLI setup wizard, you configure the management address and gateway for the device during initial system configuration. If you use the FDM-managed setup wizard, the management address and gateway remain the defaults.

If necessary, you can change these addresses through an FDM-managed device. You can also change the management address and gateway in the CLI using the **configure network ipv4 manual** and **configure network ipv6 manual** commands.

You can define static addresses, or obtain an address through DHCP if another device on the management network is acting as a DHCP server. By default, the management address is static, and a DHCP server runs on the port (except for Virtual FDM-Managed Device, which does not have a DHCP server). Thus, you can plug a device directly into the management port and get a DHCP address for your workstation. This makes it easy to connect to and configure the device.

Caution If you change the address to which you are currently connected, you will lose access to the FDM-managed device (or the CLI) when you save the changes, as they are applied immediately. You will need to reconnect to the device. Ensure that the new address is valid and available on the management network.

Procedure

Step 1 Configure the management IP address, network mask or IPv6 prefix, and gateway (if necessary) for IPv4, IPv6, or both. You must configure at least one set of properties. Leave one set blank to disable that addressing method.

Step 2 Select **Type** > **DHCP** to obtain the address and gateway through DHCP or IPv6 auto configuration. However, you cannot use DHCP if you are using the data interfaces as the gateway. In this case, you must use a static address.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Hostname

You can change the device hostname.

Procedure

Step 1 In the **Firewall Hostname** field, enter a new hostname for the device.

Step 2 Click **Save**.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure NTP Server

Configure Network Time Protocol (NTP) servers to set the time on the system.

Procedure

Step 1 Select whether you want to use your own (manual) or Cisco's time servers.

- **New NTP Server**. Enter the fully qualified domain name or IP address of the NTP server you want to use. For example, ntp1.example.com or 10.100.10.10.
- **Use Default**.

Step 2 Click **Save.**

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure URL Filtering

The system obtains the URL category and reputation database from Cisco Collective Security Intelligence (CSI). These preferences control database updates and how the system handles URLs with unknown category or reputation. You must enable the URL Filtering license to set these preferences.

Caution You can configure URL Filtering Preferences if you do not have a URL Smart License, but you need the smart license to deploy. You will be blocked from deploying until you add a URL Smart License.

Procedure

Step 1 Enable the applicable options:

- Click the **Enable Automatic Updates** slider On to automatically check for and download updated URL data, which includes category and reputation information. After you deploy, the FDM-managed device checks for updates every 30 minutes.
- Click the **Query Cisco CSI for Unknown URLs** slider to ON to check the Cisco CSI for updated information on URLs that do not have category and reputation data in the local URL filtering database.
- **URL Time to Live** is only in effect if you enable the **Query Cisco CSI for Unknown URLs** option. This determines how long to cache the category and reputation lookup values for a given URL. When the time to live expires, the next attempted access of the URL results in a fresh category/reputation lookup. A shorter time results in more accurate URL filtering, a longer time results in better performance for unknown URLs. The default selection is **Never**.

Step 2 Click **Save**.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Cloud Services

Use the Cloud Services page to manage cloud-based services.

Note Connecting to the Cisco Success Network and configuring which events are sent to the Cisco cloud are features that can be configured on FDM-managed devices running software versions 6.6 and higher.

Connecting to the Cisco Success Network

By enabling Cisco Success Network, you are providing usage information and statistics to Cisco that are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

When you enable the connection, your device establishes a secure connection to the Cisco Cloud so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times.

Before you begin

To enable Cisco Success Network the device must be enrolled with the cloud using an FDM-managed device. To enroll the device either register the device with Cisco Smart Software Manager (on the Smart Licensing page) or enroll with Security Cloud Control by entering a registration key.

Attention If you enable Cisco Success Network on the active unit in a high availability group, you are also enabling the connection on the standby unit.

Procedure

Step 1 Click the **Cloud Services** tab.

Step 2 Click the **Enabled** slider for the Cisco Success Network feature to change the setting as appropriate.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Sending Events to the Cisco Cloud

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered.

Before you begin

You must register the device with the Cisco Smart Software Manager before you can enable this service.

You can connect to the Cisco Threat Response at https://visibility.amp.cisco.com/ in the US region, https://visibility.amp.cisco.com/ in the EU region. You can watch videos about the use and benefits of the application on YouTube at http://cs.co/CTRvideos. For more information about using Cisco Threat Response with FTD, see *Firepower and CTR Integration Guide*, which you can find at https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Procedure

Step 1 Click the **Cloud Services** tab.

Step 2 Click the **Enabled** slider for the **Send Events to the Cisco Cloud** option to change the setting as appropriate.

Step 3 When you are enabling the service, you are prompted to select the events to send to the cloud.

- **File/Malware** - For any file policies, you have applied in any access control rule.
- **Intrusion Events** - For any intrusion policies, you have applied in any access control rule.
- **Connection Events** - For access control rules where you have enabled logging. When you select this option, you can also elect to send All Connection Events, or only send the High Priority connection events. High-priority connection events are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies.

Step 4 Click **Save**.

Step 5 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Enabling or Disabling Web Analytics

Enabling web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted. You can use Security Cloud Control to configure this feature on all versions of FDM-managed device.

Web analytics is enabled by default.

Procedure

Step 1 Click the **Web Analytics** tab.

Step 2 Click the **Enable** slider for the **Web Analytics** feature to change the setting as appropriate.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Security Cloud Control Command Line Interface

Security Cloud Control provides users with a command line interface (CLI) for managing , FDM-managed threat defense devices. Users can send commands to a single device or to multiple devices simultaneously.

Related Information:

- For FTD CLI documentation, see Cisco Firepower Threat Defense Command Reference. Note that FDM-managed devices have limited CLI functionality. These devices only have the following commands: `show, ping, traceroute, packet-tracer, failover, and shutdown.`

Using the Command Line Interface

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Use the device tabs and filter button to find the device you want to manage using the command line interface (CLI).

Step 4 Select the device.

Step 5 In the **Device Actions** pane, click **>_Command Line Interface.**

Step 6 Click the **Command Line Interface** tab.

Step 7 Enter your command, or commands, in the command pane and click **Send.** The device's response to the command(s) are displayed below in the "response pane."

Note If there are limitations on the commands you can run, those limitations are listed above the command pane.

Related Topics

Entering Commands in the Command Line Interface, on page 544

Entering Commands in the Command Line Interface

A single command can be entered on a single line or several commands can be entered sequentially on several lines and Security Cloud Control will execute them in order. The following ASA example sends a batch of commands which creates three network objects and a network object group that contains those network objects.

Entering FDM-managed device Commands: The CLI console uses the base Threat Defense CLI. You cannot enter the diagnostic CLI, expert mode, or FXOS CLI (on models that use FXOS) using the CLI console. Use SSH if you need to enter those other CLI modes.

Work with Command History

After you send a CLI command, Security Cloud Control records that command in the history pane on the **Command Line Interface** page. You can rerun the commands saved in the history pane or use the commands as a template:

Procedure

Step 1 In the left pane, click **Security Devices** page.

Step 2 Click the **Devices** tab to locate the device.

Step 3 Click the appropriate device type tab.

Step 4 Click **>_Command Line Interface**.

Step 5 Click the clock icon to expand the history pane if it is not already expanded.

Step 6 Select the command in the history pane that you want to modify or resend.

Step 7 Reuse the command as it is or edit it in the command pane and click **Send**. Security Cloud Control displays the results of the command in the response pane.

Note Security Cloud Control displays the `Done!` message in the response pane in two circumstances:

- After a command has executed successfully.
- When the command has no results to return. For example, you may issue a show command with a regular expression searching for a configuration entry. If there is no configuration entry that meets the criteria of the regular expression, Security Cloud Control returns `Done!`.

Bulk Command Line Interface

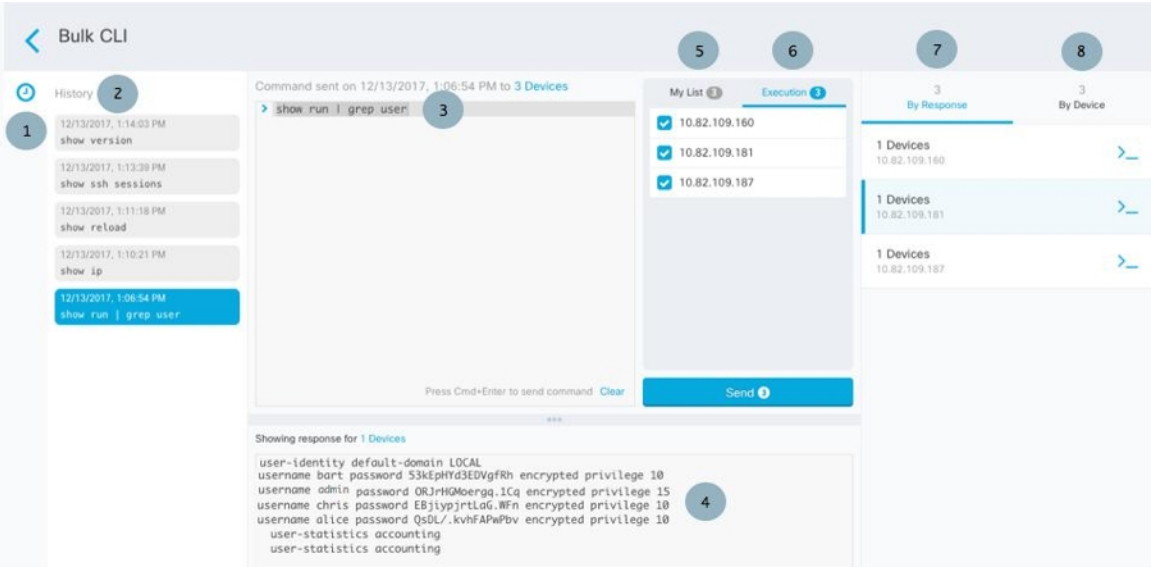
Security Cloud Control offers users the ability to manage Secure Firewall ASA, FDM-managed Threat Defense, SSH, and Cisco IOS devices using a command-line interface (CLI). Users can send commands to a single device or to multiple devices of the same kind simultaneously. This section describes sending CLI commands to multiple devices at once.

Related Information:

- For FDM-managed device documentation, Security Cloud Control supports only the base FTD CLI. These devices only have the following commands: `show, ping, traceroute, packet-tracer, failover, and shutdown`.

  For Threat Defense CLI documentation, see Cisco Firepower Threat Defense Command Reference.

Bulk CLI Interface



Note Security Cloud Control displays the **Done!** message in two circumstances:

- After a command has executed successfully without errors.
- When the command has no results to return. For example, you may issue a show command with a regular expression searching for a certain configuration entry. If there is no configuration entry that meets the criteria of the regular expression, Security Cloud Control returns **Done!**.

Number	Description
1	Click the clock to expand or collapse the command history pane.
2	Command history. After you send a command, Security Cloud Control records the command in this history pane so you can return to it, select it, and run it again.
3	Command pane. Enter your commands at the prompt in this pane.
4	Response pane. Security Cloud Control displays the device's response to your command as well as Security Cloud Control messages. If the response was the same for more than one device, the response pane displays the message "Showing Responses for X devices." Click X devices and Security Cloud Control displays all the devices that returned the same response to the command. **Note** Security Cloud Control displays the **Done!** message in two circumstances: • After a command has executed successfully without errors. • When the command has no results to return. For example, you may issue a show command with a regular expression searching for a certain configuration entry. If there is no configuration entry that meets the criteria of the regular expression, Security Cloud Control returns **Done!**.
5	**My List** tab displays the devices you chose from the **Inventory** table and allows you to include or exclude devices you want to send a command to.
6	The **Execution** tab, highlighted in the figure above, displays the devices in the command that is selected in the history pane. In this example, the show run | grep user command is selected in the history pane and the Execution tab shows that it was sent to 10.82.109.160, 10.82.109.181, and 10.82.10.9.187.
7	Clicking the **By Response** tab shows you the list of responses generated by the command. Identical responses are grouped together in one row. When you select a row in the By Response tab, Security Cloud Control displays the response to that command in the response pane.
8	Clicking the **By Device** tab displays individual responses from each device. Clicking one of the devices in the list allows you to see the response to the command from a specific device.

Send Commands in Bulk

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the devices.

Step 3 Select the appropriate device tab and use the filter button to find the devices you want to configure using the command line interface.

Step 4 Select the devices.

Step 5 in the **Device Actions** pane, click **>_Command Line Interface**.

Step 6 You can check or uncheck devices you want to send the commands to in the **My List** field.

Step 7 Enter your commands in the command pane and click **Send**. The command output is displayed in the response pane, the command is logged in the Change Log, and the command Security Cloud Control records your command in the History pane in the Bulk CLI window.

Work with Bulk Command History

After you send a bulk CLI command, Security Cloud Control records that command in the Bulk CLI Interface history page. You can rerun the commands saved in the history pane or use the commands as a template. The commands in the history pane are associated with the original devices on which they were run.

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate devices.

Step 3 Click the appropriate device type tab and click the filter icon to find the devies you want to configure.

Step 4 Select the devices.

Step 5 Click **Command Line Interface**.

Step 6 **Select** the command in the History pane that you want to modify or resend. Note that the command you pick is associated with specific devices and not necessarily the ones you chose in the first step.

Step 7 Look at the My List tab to make sure the command you intend to send will be sent to the devices you expect.

Step 8 Edit the command in the command pane and click **Send**. Security Cloud Control displays the results of the command in the response pane.

Work with Bulk Command Filters

After you run a bulk CLI command you can use the **By Response** filter and the **By Device** filter to continue to configure the devices.

By Response Filter

After running a bulk command, Security Cloud Control populates the **By Response** tab with a list of responses returned by the devices that were sent the command. Devices with identical responses are consolidated in a single row. Clicking a row in the **By Response** tab displays the response from the device(s) in the response pane. If the response pane shows a response for more than one device, it displays the message "Showing Responses for X devices." Click **X devices** and Security Cloud Control displays all the devices that returned the same response to the command.

To send a command to the list of devices associated with a command response, follow this procedure:

Procedure

Step 1 Click the command symbol in a row in the **By Response** tab.

Step 2 Review the command in the command pane and click **Send** to resend the command or click **Clear** to clear the command pane and enter a new command to send to the devices and then click **Send**.

Step 3 Review the responses you receive from your command.

Step 4 If you are confident that the running configuration file on the devices you chose reflects your change, type `write memory` in the command pane and click **Send**. This saves your running configuration to the startup configuration.

By Device Filter

After running a bulk command, Security Cloud Control populates the the Execution tab and the **By Device** tab with the list of devices that were sent the command. Clicking a row in the **By Device** tab displays the response for each device.

To run a command on that same list of devices, follow this procedure:

Procedure

Step 1 Click the **By Device** tab.

Step 2 Click **>_Execute a command on these devices**.

Step 3 Click **Clear** to clear the command pane and enter a new command.

Step 4 In the My List pane, specify the list of devices you want to send the command to by checking or unchecking individual devices in the list.

Step 5 Click **Send**. The response to the command is displayed in the response pane. If the response pane shows a response for more than one device, it displays the message "Showing Responses for X devices." Click X devices and Security Cloud Control displays all the devices that returned the same response to the command.

Step 6 If you are confident that the running configuration file on the devices you chose reflects your change, type `write memory` in the command pane and click **Send**.

Command Line Interface Macros

A CLI macro is a fully-formed CLI command ready to use, or a template of a CLI command you can modify before you run it. All macros can be run on one or more FTD devices simultaneously.

Use CLI macros that resemble templates to run the same commands on multiple devices at the same time. CLI macros promote consistency in your device configurations and management. Use fully-formed CLI macros to get information about your devices. There are different CLI macros that are immediately available for you to use on your FTD devices.

You can create CLI macros for monitoring tasks that you perform frequently. See Create a CLI Macro from a New Command for more information.

CLI macros are system-defined or user-defined. System-defined macros are provided by Security Cloud Control and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted.

Note You can only create macros for a device once it has been onboarded to Security Cloud Control.

Using the ASA as an example, if you want to find a particular user on one of your ASAs, you could run this command:

```
show running-config | grep username
```

When you run the command, you would replace *username* with the username of the user you are searching for. To make a macro out of this command, use the same command and put curly braces around *username.*

```
> show running-config | grep {{username}}
```

You can name your parameters anything you want. You can also create the same macro with this parameter name:

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

The parameter name can be descriptive and must use alphanumeric characters and underlines. The command syntax, in this case the

```
show running-config | grep
```

part of the command, must use proper CLI syntax for the device you are sending the command to.

Create a CLI Macro from a New Command

Procedure

Step 1 Before you create a CLI macro, test the command in Security Cloud Control's Command Line Interface to make sure the command syntax is correct and it returns reliable results.

Note
- For FDM-managed devices, Security Cloud Control supports only the commands that can be run in FDM's CLI console: `show`, `ping`, `traceroute`, `packet-tracer`, `failover`, `reboot`, and `shutdown`. See Cisco Firepower Threat Defense Command Reference for a full description of the syntax of those commands.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device.

Step 4 Click the appropriate device type tab and select an online and synced device.

Step 5 Click **>_Command Line Interface.**

Step 6 Click the CLI macro favorites star to see what macros already exist.

Step 7 Click the the plus button .

Step 8 Give the macro a unique name. Provide a description and notes for the CLI macro if you wish.

Step 9 Enter the full command in the **Command** field.

Step 10 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 11 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a CLI Macro.

Create a CLI Macro from CLI History or from an Existing CLI Macro

In this procedure, you are going to create a user-defined macro from a command you have already run, another user-defined macro, or from a system-defined macro.

Procedure

Step 1 In the left pane, **Security Devices**.

Note If you want to create a user-defined macro from CLI history, select the device on which you ran the command. CLI macros are shared across devices on the same account but not CLI history.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select an online and synced device.

Step 4 Click **>_Command Line Interface.**

Step 5 Find the command you want to make a CLI macro from and select it. Use one of these methods:

- Click the clock to view the commands you have run on that device. Select the one you want to turn into a macro and the command appears in the command pane.
- Click the CLI macro favorites star to see what macros already exist. Select the user-defined or system-defined CLI macro you want to change. The command appears in the command pane.

Step 6 With the command in the command pane, click the CLI macro gold star . The command is now the basis for a new CLI macro.

Step 7 Give the macro a unique name. Provide a description and notes for the CLI macro if you wish.

Step 8 Review the command in the Command field and make the changes you want.

Step 9 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 10 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a CLI Macro.

Run a CLI Macro

Procedure

Step 1 In the left pane, click **Security Devices**

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select one or more devices.

Step 4 Click **>_Command Line Interface.**

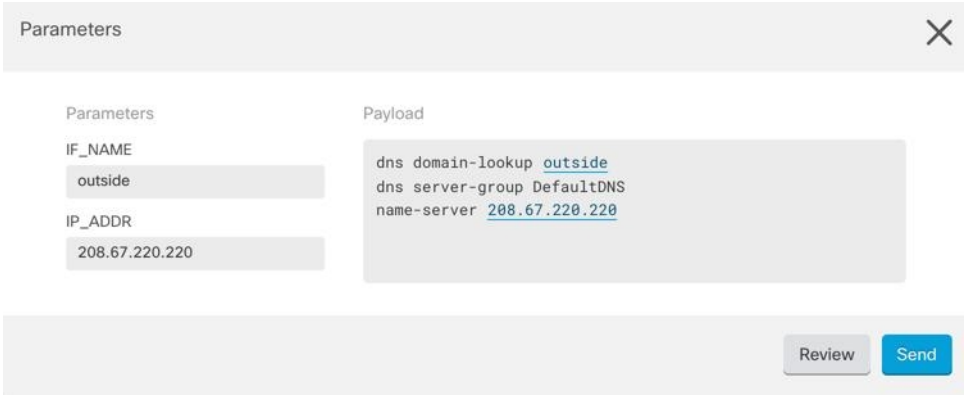
Step 5 In the command panel, click the star .

Step 6 Select a CLI macro from the command panel.

Step 7 Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Configure DNS macro below, click **>_ View Parameters.**

Step 8 In the Parameters pane, fill in the values for the parameters in the Parameters fields.



Step 9 Click **Send**. After Security Cloud Control has successfully, sent the command and updated the device's configuration, you receive the message, Done!

- For an FTD, the device's active configuration is updated.

Step 10 After you send the command you may see the message, "Some commands may have made changes to the running config" along with two links.

- Clicking **Write to Disk** saves the changes made by this command, and any other change that in the running config, to the device's startup config.
- Clicking **Dismiss**, dismisses the message.

Edit a CLI Macro

You can edit user-defined CLI macros but not system-defined macros. Editing a CLI macro changes it for all your FTD devices. Macros are not specific to a particular device.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select your device.

Step 5 Click **Command Line Interface**.

Step 6 Select the user-defined macro you want to edit.

Step 7 Click the edit icon in the macro label.

Step 8 Edit the CLI macro in the Edit Macro dialog box.

Step 9 Click **Save**.

See Run a CLI Macro for instructions on how to run the CLI macro.

Delete a CLI Macro

You can delete user-defined CLI macros but not system-defined macros. Deleting a CLI macro deletes it for all your devices. Macros are not specific to a particular device.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select your device.
Step 5 Click >_**Command Line Interface**.
Step 6 Select the user-defined CLI macro you want to delete.
Step 7 Click the trash can icon in the CLI macro label.
Step 8 Confirm you want to remove the CLI macro.

Command Line Interface Documentation

Security Cloud Control partially supports the command line interface of the FDM-managed device. We provide a terminal-like interface within Security Cloud Control for users to send commands to single devices and multiple devices simultaneously in command-and-response form. For commands that are not supported in Security Cloud Control, access the device with a device GUI terminal, such as PuTTy or an SSH Client, and see the CLI documentation for more commands.

Export Security Cloud Control CLI Command Results

You can export the results of CLI commands issued to a standalone device, or several devices, to a comma separated value (.csv) file so you can filter and sort the information in it however you like. You can export the CLI results of a single device, or many devices at once. The exported information contains the following:

- Device
- Date
- User
- Command
- Output

Export CLI Command Results

You can export the results of commands you have just executed in the command window to a .csv file:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the **Device Actions** pane for the device, click **>_Command Line Interface**.

Step 6 In the command line interface pane, enter a command and click **Send** to issue it to the device.

Step 7 To the right of the window of entered commands, click the export icon .

Step 8 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Export the Results of CLI Macros

You can export the results of macros that have been executed in the command window. Use the following procedure to export to a .csv file, the results of CLI macros executed on one or multiple devices:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the **Device Actions** pane for the device, click **>_Command Line Interface**.

Step 6 In the left pane of the CLI window, select the CLI macro favorites star .

Step 7 Click on the macro command you want to export. Fill in any appropriate parameters and click **Send**.

Step 8 To the right of the window of entered commands, click the export icon .

Step 9 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Export the CLI Command History

Use the following procedure to export the CLI history of one or multiple devices to a .csv file:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the Device Actions pane for the device, click **>_Command Line Interface**.

Step 6 Click the **Clock** icon to expand the history pane if it is not already expanded.

Step 7 To the right of the window of entered commands, click the export icon .

Step 8 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Related Information:

- Security Cloud Control Command Line Interface, on page 543
- Create a CLI Macro from a New Command
- Delete a CLI Macro
- Edit a CLI Macro
- Run a CLI Macro
- Command Line Interface Documentation
- Bulk Command Line Interface

Export the CLI Macro List

You can only export macros that have been executed ed in the command window. Use the following procedure to export the CLI macros of one or multiple devices to a .csv file:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the Device Actions pane for the device, click **>_Command Line Interface**.

Step 6 In the left pane of the CLI window, select the CLI macro favorites star .

Step 7 Click on the macro command you want to export. Fill in any appropriate parameters and click **Send**.

Step 8 To the right of the window of entered commands, click the export icon .

Step 9 Give the .csv file a descriptive name and save the file to your local file system.

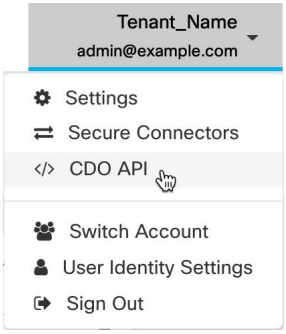
Security Cloud Control Public API

Security Cloud Control has published its public API and provided you with documentation, examples, and a playground to try things out. The goal of our public API is to provide you with a simple and effective way to perform a lot of what you would normally be able to do in the Security Cloud Control UI, but in code.

To use this API, you will need to know GraphQL. Their official guide (https://graphql.org/learn/) provides a thorough, light read.

To find the full schema documentation, go to the GraphQL Playground, and click the docs tab on the right side of the page.

You can launch the Security Cloud Control Public API by selecting it from the user menu.



Create a REST API Macro

Using the API Tool

Security Cloud Control provides the API Tool interface to execute the FDM-managed device REpresentational State Transfer (REST) Application Programming (API) requests for performing advanced actions on an FDM-managed device. The REST API uses JavaScript Object Notation (JSON) format to represent objects.

The interface provides system-defined or user-defined API macros. System-defined macros are provided by Security Cloud Control and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted. You can use all the resource groups supported in the Secure Firewall device manager API Explorer.

Note Security Cloud Control supports only API endpoints that return JSON.

Assumption

It is assumed that you have a general knowledge of programming and a specific understanding of REST APIs and JSON. If you are new to these technologies, please first read a general guide on REST APIs.

Supported Documents

- You can refer to the Cisco Firepower Threat Defense REST API Guide for detailed information.
- You can also find reference information and examples online at Cisco DevNet Site.

Supported HTTP Methods

You can use the following HTTP methods only.

Important A user with the User Roles in Security Cloud Control role can perform only the GET operation.

Attribute	Description
GET	To read data from the device.
POST	To create new objects for a type of resource. For example, use POST to create a new network object.
PUT	To change the attributes of an existing resource. When using PUT, you must include the entire JSON object. You cannot selectively update individual attributes within an object. For example, use PUT to modify the address contained within an existing network object.
DELETE	To remove a resource that you, or another user, created. For example, use DELETE to remove a network object that you no longer use.

Related Information:

- How to Enter a Secure Firewall Threat Defense REST API Request
- About FTD REST API Macros
  - Create a REST API Macro
  - Run a REST API Macro
  - Edit a REST API Macro
  - Delete a REST API Macro

How to Enter a Secure Firewall Threat Defense REST API Request

You can select an FDM-managed device and specify a single command or execute commands that need additional parameters.

If you want to determine the syntax of a REST API request, log on to the device's API Explorer page, such as https://ftd.example.com/#/api-explorer, and click the required resource groups to see the syntax of the command to be executed. For example, https://10.10.5.84/#/api-explorer.

The following figure shows an example of a single REST API request in Security Cloud Control:

The following figure shows an example of a REST API request that needs additional parameters. You need manually specify the data in the **Request Body**. If you want to determine the syntax of a command, log on to the device's API Explorer page.

Note The device must be in the synced state to execute the POST request.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

Step 5 Select the request method from the drop-down and type**/api/fdm/latest/**and then the command that you want to execute. If you are executing a POST or PUT command, enter the request body.

Step 6 Click **Send**. The **Response Body** shows the response of the executed command.

Important The POST request usually makes changes to the staged configuration on the device. Click **Commit Changes in FDM** to send the changes to the FDM-managed device.

Related Information:

- Using the API Tool, on page 556
- About FTD REST API Macros
  - Create a REST API Macro

- Run a REST API Macro
- Edit a REST API Macro
- Delete a REST API Macro

About FTD REST API Macros

A REST API macro is a fully-formed REST API command ready to use, or a template of a REST API command you can modify before you run it. All REST API macros can be run on one or more FDM-managed devices simultaneously.

Use REST API macros that resemble templates to run the same commands on multiple devices at the same time. REST API macros promote consistency in your device configurations and management. Use fully-formed REST API macros to get information about your devices. There are different REST API macros that are immediately available for you to use on your FDM-managed devices.

You can create REST API macros for tasks that you perform frequently. See Create a REST API Macro for more information.

REST API macros are system-defined or user-defined. System-defined macros are provided by Security Cloud Control and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted.

Note You can only create macros for a device once it has been onboarded to Security Cloud Control.

Related Information:

- Create a REST API Macro
- Run a REST API Macro
- Edit a REST API Macro
- Delete a REST API Macro

Create a REST API Macro

Create a REST API Macro from a New Command

Procedure

Step 1 Before you create a REST API macro, test the command in Security Cloud Control's REST API Interface to make sure the command syntax is correct and it returns reliable results.

Note You can only create macros for a device once it has been onboarded to Security Cloud Control.

Step 2 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

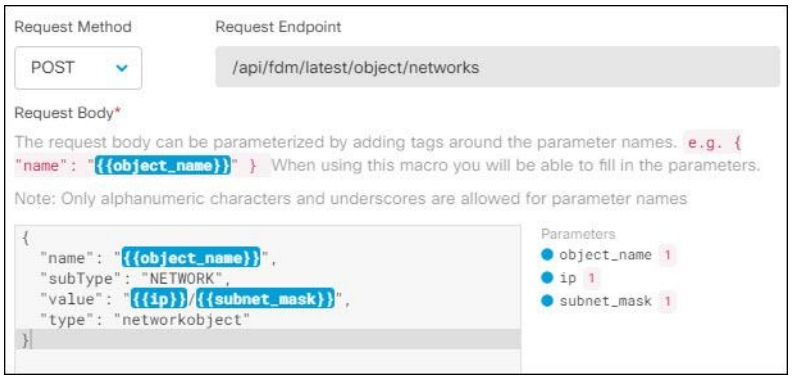
Step 3 Click the REST API macro favorites star to see what macros already exist.

Step 4 Click the plus button .

Step 5 Give the macro a unique name. Provide a description and notes for the REST API macro if you wish.

Step 6 Select a **Request Method** and enter the endpoint URL in the **Request Endpoint** field. See Cisco Firepower Threat Defense REST API Guide for detailed information.

Step 7 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.



Step 8 Click **OK**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a REST API Macro.

Create a REST API Macro from History or from an Existing REST API Macro

In this procedure, you are going to create a user-defined REST API macro from a command you have already executed, another user-defined macro, or from a system-defined macro.

Procedure

Step 1 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

Note If you want to create a user-defined macro from REST API history, select the device on which you ran the command. REST API macros are shared across devices on the same account but not REST API history.

Step 2 Find the command you want to make an API macro from and select it. Use one of these methods:

- Click the clock to view the commands you have run on that device. Double-click to select the one you want to turn into a macro and the command appears in the command pane.
- Click the API macro favorites star to see what macros already exist. Select the user-defined or system-defined API macro you want to change. The command appears in the command pane.

Step 3 With the command in the command pane, click the API macro gold star  . The command is now the basis for a new API macro.

Step 4 Give the macro a unique name. Provide a description and notes for the API macro if you wish.

Step 5 Review the command in the Command field and make the changes you want.

Step 6 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 7 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a REST API Macro.

Related Information:

About FTD REST API Macros

Run a REST API Macro

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

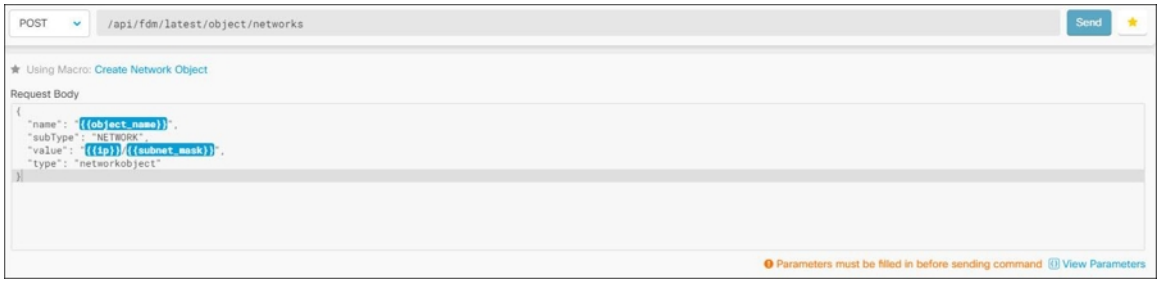
Step 4 Click **API Tool** in the **Device Actions** pane on the right.

Step 5 In the command panel, click the star ★ to view the REST API macros.

Step 6 Select a REST API macro from the command panel.

Step 7 Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Create Network Object macro below, click **View Parameters.**



Step 8 In the **Parameters** pane, fill in the values for the parameters in the Parameters fields.

Step 9 Click **Send**.

Note The FDM-managed device's active configuration is updated.

Related Information:

About FTD REST API Macros

Edit a REST API Macro

You can edit user-defined REST API macros but not system-defined macros. Editing a REST API macro changes it for all your FDM-managed devices. Macros are not specific to a particular device.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

Step 5 Select the user-defined macro you want to edit.

Step 6 Click the edit icon in the macro label.

Step 7 Edit the REST API macro in the Edit Macro dialog box.

Step 8 Click **Save**.

See Run a REST API Macro for instructions on how to run the REST API macro.

Related Information:

About FTD REST API Macros

Delete a REST API Macro

You can delete user-defined REST API macros but not system-defined macros. Deleting a REST API macro deletes it for all your devices. Macros are not specific to a particular device.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select a device and in **Device Actions** on the right, click **API Tool**.

Step 5 Select the user-defined REST API macro you want to delete.

Step 6 Click the trash can icon in the REST API macro label.

Step 7 Confirm you want to remove the REST API macro.

Related Infomration:

About FTD REST API Macros

About Device Configuration Changes

In order to manage a device, Security Cloud Control must have its own copy of the device's configuration stored in its local database. When Security Cloud Control "reads" a configuration from a device it manages, it takes a copy of the device's configuration and saves it. The first time Security Cloud Control reads and saves a copy of a device's configuration is when the device is onboarded. These choices describe reading a configuration for different purposes:

- **Discard Changes**: This action is available when a device's configuration status is "Not Synced." In the Not Synced state, there are changes to the device's configuration pending on Security Cloud Control. This option allows you to undo all pending changes. The pending changes are deleted and Security Cloud Control overwrites its copy of the configuration with copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device's configuration status is Synced. Clicking Checking for Changes directs Security Cloud Control to compare its copy of the device's configuration with the copy of the configuration stored on the device. If there is a difference, Security Cloud Control immediately overwrites its copy of the device's configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, Security Cloud Control checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click Review Conflict allows you to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites Security Cloud Control's copy of a device's configuration with the latest copy of the configuration stored on the device. Security Cloud Control does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

Read All: This is a bulk operation. You can select more than one device, in any state, and click **Read All** to overwrite all the devices' configurations stored on Security Cloud Control with the configurations stored on the devices.

- **Deploy Changes**: As you make changes to a device's configuration, Security Cloud Control saves the changes you make to its own copy of the configuration. Those changes are "pending" on Security Cloud Control until they are deployed to the device. When there are changes to a device's configuration that have not been deployed to the device, the device is in the Not Synced configuration state.

  Pending configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an effect. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device. Deployments can be initiated for a single device or on more than one device simultaneously.

- **Discard All** is an option that is only available after you click **Preview and Deploy...**. After clicking Preview and Deploy, Security Cloud Control shows you a preview of the pending changes in Security Cloud Control. Clicking **Discard All** deletes all pending changes from Security Cloud Control and does not deploy anything to the selected device(s). Unlike "Discard Changes" above, deleting the pending changes is the end of the operation.

Note You can schedule deployments or recurring deployments. See Schedule an Automatic Deployment, on page 572 for more information.

Read All Device Configurations

If a configuration change is made to a device outside of Security Cloud Control, the device's configuration stored on Security Cloud Control and the device's local copy of its configuration are no longer the same. You many want to overwrite Security Cloud Control's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

See About Device Configuration Changes for more information about how Security Cloud Control manages the two copies of the device's configuration.

Here are three configuration statuses where clicking **Read All** will overwrite Security Cloud Control's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**-If conflict detection is enabled, Security Cloud Control polls the devices it manages every 10 minutes for changes made to their configurations. If Security Cloud Control finds that the configuration on the device has changed, Security Cloud Control displays a "Conflict detected" configuration status for the device.

- **Synced**-If the device is in a synced state, and you click **Read All**, Security Cloud Control immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, Security Cloud Control confirms your intent to overwrite its copy of the device's configuration and then Security Cloud Control performs the overwrite.

- **Not Synced**-If the device is in the Not Synced state, and you click **Read All**, Security Cloud Control warns you that there are pending changes made to to the device's configuration using Security Cloud Control and that proceeding with the Read All operation will delete those changes and then overwrite

Security Cloud Control's copy of the configuration with the configuration on the device. This Read All functions like Discard Configuration Changes.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 (Optional) Create a Change Request Management to identify the results of this bulk action easily in the Change Log.

Step 5 Select the devices whose configurations you want to save Security Cloud Control. Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Click **Read All**.

Step 7 Security Cloud Control warns you if there are configuration changes staged on Security Cloud Control, for any of the devices you selected, and asks if you want to continue with the bulk reading configurations action. Click **Read All** to continue.

Step 8 Look at the Monitor Jobs in Security Cloud Control for the progress of the Read All configurations operation. If you want more information about how individual actions in the bulk operation succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in Security Cloud Control.

Step 9 If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Related Information

- About Device Configuration Changes
- Discard Configuration Changes
- Check for Configuration Changes

Read Configuration Changes from FDM-Managed Device to Security Cloud Control

Why Does Security Cloud Control Read FDM-managed device Configurations?

In order to manage an FDM-managed device, Security Cloud Control must have its own stored copy of the FDM-managed device's configuration. When Security Cloud Control reads a configuration from an FDM-managed device, it takes a copy of the FDM-managed device's deployed configuration and saves it to its own database. The first time Security Cloud Control reads and saves a copy of the device's configuration file is when the device is onboarded. See About Device Configuration Changes for more information.

Pending and Deployed Changes

Configuration changes made to the FDM-managed device directly through the Firepower Device Manager (FDM) or its CLI are referred to as staged changes on the FDM-managed device until they are deployed. A

staged, or pending, change can be edited or deleted without having any affect on traffic running through the FDM-managed device. Once the pending changes are deployed, however, they are enforced by the FDM-managed device and affect traffic running through the device.

Conflict Detected

If you enable Conflict Detection on the device, Security Cloud Control checks for configuration changes every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status. If you do **not** have Conflict Detection enabled, or a change has been made to the device's configuration within the 10 minute interval between automatic polling, clicking **Check for Changes** prompts Security Cloud Control to immediately compare the copy of the configuration on the device with the copy of the configuration stored on Security Cloud Control. You can choose to **Review Conflict** to examine the differences between the device configuration and the configuration saved to Security Cloud Control, then select **Discard Changes** to remove the staged changes and revert to the saved configuration or confirm the changes. You can also choose to **Accept without Review**; this option takes the configuration and overwrites what is currently saved to Security Cloud Control.

Discard Changes Procedure

To discard configuration changes from the FDM-managed device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appopriate device type tab.

Step 4 Select the device whose configuration is set to Conflict Detected and gives you the link to Revert Pending Changes. The message explains that you can click the link to revert pending changes or you can log on to the device using the local manager FDM and deploy the changes first. You can use Filters to find the device in a conflict state.

Caution Clicking the Revert Pending Changes link deletes pending changes on FDM-managed device immediately. You are not given an opportunity to review the changes first.

Step 5 Review the changes on FDM before clicking Revert Pending Changes:

a. Open a browser window and enter https://<*IP_address_of_the_FTD*>.

b. Look for the deployment icon in FDM. It will have an orange circle indicating that there are changes ready to deploy  .

c. Click the icon and review the pending changes:

- If the changes can be deleted, return to Security Cloud Control and click "Revert Pending Changes." At this point, the configuration on the FDM-managed device and the copy of the configuration on Security Cloud Control should be the same. You are done.
- If you want to deploy the changes to the device, click **Deploy Now**. Now the deployed configuration on the FDM-managed device and the configuration on stored on Security Cloud Control are different. You

can then return to Security Cloud Control and Check for Configuration Changes. Security Cloud Control identifies identifies that there has been a change on the FDM-managed device, and gives you an opportunity to review the conflict. See Conflict Detection to resolve that state.

If Reverting Pending Changes Fails

Changes to the system databases and security feeds can't be reverted by Security Cloud Control. Security Cloud Control recognizes that there are pending changes, attempts to revert them and then fails. To determine if the revert failure is due to pending database updates or security feed updates, log into the device's FDM console. It will have an orange circle indicating that there are changes ready to deploy  . Click the deploy button to review the pending changes and deploy them or discard them as is appropriate.

Review Conflict Procedure

To review configuration changes from the FDM-managed device, follow this procedure:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device whose configuration is marked Conflict Detected and gives you a link to **Review Conflict** in the Conflict Detected pane on the right.

Step 5 Click **Review Conflict.**

Step 6 Compare the two configurations presented to you.

Step 7 Take one of these actions:

- Click **Accept** to overwrite the last known configuration on Security Cloud Control with the one found on the device. **Note**: The entire configuration stored on Security Cloud Control will be completely overwritten by the configuration found on the device.
- Click **Reject** to reject the changes made on the device and replace them with the last known configuration on Security Cloud Control.
- Click **Cancel** to stop the action.

Note You can prompt Security Cloud Control to immediately check a device for an out-of-band change by clicking Check for Configuration Changes while the device is in the Synced state.

Accept Without Review Procedure

To accept configuration changes from the FDM-managed device without reviewing, follow this procedure:

Procedure

Step 1 In the left pane, click the **Security Devices** tab.

Step 2 Click the appopriate device type tab.

Step 3 Select the device whose configuration is marked Conflict Detected and gives you a link to **Accept Without Review** in the Conflict Detected pane on the right.

Step 4 Click **Accept Without Review**. Security Cloud Control accepts and overwrites the current configuration.

Related Information:

- About Device Configuration Changes
- Conflict Detection
- Discarding Changes

Preview and Deploy Configuration Changes for All Devices

Security Cloud Control informs you when you have made a configuration change to a device on your tenant, but you have not deployed that change, by displaying an orange dot on the Deploy icon  . The devices affected by these changes show the status "Not Synced" in the Devices and **Services** page. By clicking **Deploy**, you can review which devices have pending changes and deploy the changes to those devices.

Note For every new FDM or FTD network object or group that you create and make changes to, Security Cloud Control creates an entry in this page for all on-premises management centers that are managed by Security Cloud Control.

This deployment method is available for all supported devices.

You can use this deployment method for single configuration changes or wait and deploy multiple changes at once.

Procedure

Step 1 In the top right corner of the screen, click the **Deploy** icon  .

Step 2 Select the devices with changes you want to deploy. If a device has a yellow caution triangle, you can not deploy changes to that device. Hover your mouse over the yellow caution triangle to find out why you can't deploy changes to that device.

Step 3 (Optional) If you want to see more information about a pending change, click the **View Detailed Changelog** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.

Step 4 (Optional) Change Request Management to track your changes without leaving the **Devices with Pending Changes** page.

Step 5 Click **Deploy Now** to deploy the changes immediately to the devices you selected. You'll see the progress in the Active jobs indicator in the Jobs tray.

Step 6 (Optional) After the deployment has finished, click **Jobs** in the Security Cloud Control navigation bar. You will see a recent "Deploy Changes" job showing the results of the deployment.

Step 7 If you created a change request label, and you have no more configuration changes to associate with it, clear it.

What to do next

- About Scheduled Automatic Deployments
- Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device, on page 569
- Change Log Entries After Deploying to FDM-Managed Device, on page 587

Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device

Why Does Security Cloud Control Deploy Changes to an FDM-Managed Device?

As you manage and make changes to a device's configuration with Security Cloud Control, Security Cloud Control saves the changes you make to its own copy of the configuration file. Those changes are considered staged on Security Cloud Control until they are deployed to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an affect on the traffic running through the device. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not not overwrite the entire configuration file stored on the device.

Like Security Cloud Control, FDM-managed device has the concept of pending changes and deployed changes. Pending changes on FDM-managed device are the equivalent of staged changes on Security Cloud Control. A pending change can be edited or deleted without having any affect on traffic running through the FDM-managed device. Once the pending changes are deployed, however, they are enforced by the FDM-managed device and affect traffic running through the device.

Because of FDM-managed devices two step process for editing configuration files, Security Cloud Control deploys changes to an FDM-managed device slightly differently than it does to other devices it manages. Security Cloud Control first deploys the changes to FDM-managed device and the changes are in the pending state. Then, Security Cloud Control deploys the changes on the devices and they become live. Now that the changes have been deployed, they are enforced and affect traffic running through the FDM-managed device. This applies to both standalone and high availability (HA) devices.

Deployments can be initiated for a single device or on more than one device simultaneously. You can schedule individual deployments or recurring deployments for a single device.

Two things will prevent Security Cloud Control from deploying changes to an FDM-managed device:

- If there are staged changes on the FDM-managed device. See Conflict Detection for more information on how to resolve this state.
- Security Cloud Control does not deploy changes if there are changes in the process of being deployed to the FDM-managed device.

Scheduling Automatic Deployments

You can also configure your tenant to schedule deployments to a single device with pending changesAbout Scheduled Automatic Deployments.

Deploy Changes to a Device

Procedure

Step 1 After you make a configuration change for a device using Security Cloud Control and save it, that change is saved in Security Cloud Control instance of the device's configuration.

Step 2 In the navigation bar, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab. You should see that the configuration status of the device you made changes to is now "Not synced."

Step 5 Deploy the changes using one of these methods:

- Select the device and in the Not Synced pane on the right, click **Preview and Deploy.** On the Pending Changes screen, review the changes. If you are satisfied with the pending version, click **Deploy Now**. After the changes are deployed successfully, you can view the Manage Change Logs in Security Cloud Control to confirm what just happened.
- Click the **Deploy** icon at the top-right of the screen. See Preview and Deploy Configuration Changes for All Devices, on page 568 for more information.

Cancelling Changes

If, when deploying a change from Security Cloud Control to a device, you click **Cancel**, the changes you made are not deployed to the device. The process is canceled. The changes you made are still pending on Security Cloud Control and can be edited further before you finally deploy them to FDM-managed device.

Discarding Changes

If, when previewing changes, you click **Discard all**, the changes you made, and any other changes any other user made but did not deploy to the device, are deleted. Security Cloud Control reverts its pending configuration to the last read or deployed configuration before any changes were made.

Bulk Deploy Device Configurations

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select all of the devices for which you have made configuration changes on Security Cloud Control. These devices should show "Not Synced" status.

Step 5 Deploy the changes using one of these methods:

- Click the button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

  Note If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

- Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.

Step 6 (Optional) Click the Jobs icon  in the navigation bar to view the results of the bulk deploy.

Related Information:

- Schedule an Automatic Deployment, on page 572

About Scheduled Automatic Deployments

Using Security Cloud Control, you can make configuration changes to one or more of the devices it manages and then schedule the changes to be deployed to those devices at a time that is convenient for you.

You can only schedule deployments if you Enable the Option to Schedule Automatic Deployments, on page 51 in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments. A scheduled deployment deploys all the staged changes saved on Security Cloud Control at the date and time set. You can also view and delete scheduled deployments from the Jobs page.

If there were changes made directly to the device that have not been About Device Configuration Changes to Security Cloud Control, the scheduled deployment will be skipped until that conflict is resolved. The Jobs

page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

Caution If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

Note When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

Schedule an Automatic Deployment

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window. Follow this procedure to schedule a one-time or a recurring deployment for a single device:

Note If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one ore more devices.

Step 5 In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.

Step 6 Select when the deployment should occur.

- For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
- For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.

Step 7 Click **Save**.

Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one or more devices.

Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .

Step 6 Edit the recurrence, date, or time of a scheduled deployment.

Step 7 Click **Save**.

Delete a Scheduled Deployment

Follow this procedure to delete a scheduled deployment:

Note If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one or more devices.

Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Delete** .

What to do next

- About Device Configuration Changes
- Read All Device Configurations, on page 564
- Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device, on page 569
- Preview and Deploy Configuration Changes for All Devices, on page 568

Check for Configuration Changes

Check for Changes to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on Security Cloud Control. You will see the this option when the device is in the "Synced" state.

To check changes:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device, whose configuration you suspect may have been changed directly on the device.

Step 5 Click **Check for Changes** in the Synced pane on the right.

Step 6 The behavior that follows is slightly different depending on the device:

- For FTD device if there has been a change to the device's configuration, you will receive the message:

```
Reading the policy from the device. If there are active deployments on the device,
reading will start after they are finished.
```

  - Click **OK** to continue. The configuration on the device will overwrite the stored configuration on Security Cloud Control.
  - Click **Cancel** to cancel the action.

- For device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on Security Cloud Control. The configuration labeled **Found on Device** is the configuration saved on the ASA.

b. Select either:

1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."
2. **Accept** the out-of-band changes to overwrite the device's configuration stored in Security Cloud Control with the configuration found on the device.

c. Click **Continue**.

Discard Configuration Changes

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using Security Cloud Control. When you click **Discard Changes**, Security Cloud

Control *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on Security Cloud Control will be the same as the copy of the configuration on the device and the configuration status in Security Cloud Control will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you have been making configuration changes to.

Step 5 Click **Discard Changes** in the **Not Synced** pane on the right.

- For FDM-managed devices-Security Cloud Control warns you that "Pending changes on Security Cloud Control will be discarded and the Security Cloud Control configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-Security Cloud Control deletes the change immediately.
- For AWS devices-Security Cloud Control displays what you are about to delete. Click **Accept** or **Cancel**.

Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using Security Cloud Control. These changes may be made using the device's command-line interface over an SSH connection or by using a local manager like the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Premises Firewall Management Center on the On-Premises Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

Detecting Out-of-Band Changes on Devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Premises Firewall Management Center, Security Cloud Control checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of Security Cloud Control.

If Security Cloud Control finds that there are changes to the device's configuration that are not stored on Security Cloud Control, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Security Cloud Control detects a conflict, one of two conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to Security Cloud Control's database.

- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.
- In the case of an On-Premises Firewall Management Center, there may be changes made, for instance, to objects outside Security Cloud Control, which are pending to be synchronized with Security Cloud Control or changes made in Security Cloud Control which are pending to be deployed to the On-Premises Firewall Management Center.

Synchronizing Configurations Between Security Cloud Control and Device

About Configuration Conflicts

In the **Security Devices** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Premises Firewall Management Center that you manage using Security Cloud Control, navigate **Tools & Services** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Security Cloud Control) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device. Deploying your changes from Security Cloud Control to the device changes the configuration on the device to match Security Cloud Control's version.
- Changes made to devices outside of Security Cloud Control are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on Security Cloud Control to match the configuration on the device.

Conflict Detection

When conflict detection is enabled, Security Cloud Control polls the device for the default interval to to determine if a change has been made to the device's configuration outside of Security Cloud Control. If Security Cloud Control detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of Security Cloud Control are called "out-of-band" changes.

In the case of an On-Premises Firewall Management Center that is managed by Security Cloud Control, if there are changes that are staged and the device is in **Not Synced** state, Security Cloud Control stops polling the device to check for changes. When there are changes made outside Security Cloud Control which are pending to be synchronized with Security Cloud Control and changes made in Security Cloud Control which are pending to be deployed to the on-premises management center, Security Cloud Control declares the on-premises management center to be in the **Conflict Detected** state.

Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule Polling for Device Changes, on page 580 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Security Cloud Control.

Procedure

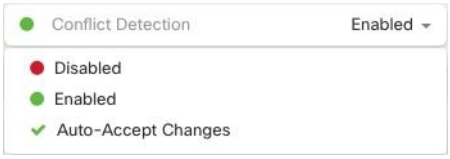
Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Select the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



Automatically Accept Out-of-Band Changes from your Device

You can configure Security Cloud Control to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using Security Cloud Control are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

The auto-accept changes feature is an enhancement to conflict detection. If you have auto-accept changes enabled on your device, Security Cloud Control checks for changes every 10 minutes to determine if there have been any out-of-band changes made to the device's configuration. If there have been configuration changes, Security Cloud Control automatically updates its local version of the device's configuration without prompting you.

Security Cloud Control will ***not*** automatically accept a configuration change if there are configuration changes made on Security Cloud Control that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Security Devices** page; then, you enable auto-accept changes for individual devices.

If you want Security Cloud Control to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection, on page 576 instead.

Configure Auto-Accept Changes

Procedure

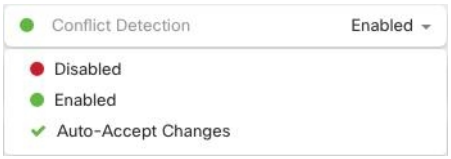
Step 1 Log in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 In the left pane, click **Administration** > **General Settings**.

Step 3 In the **Tenant Settings** area, click the toggle to **Enable the option to auto-accept device changes**. This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Security Devices** page.

Step 4 In the left pane, click **Security Devices** and select the device for which you want to automatically accept out-of-band changes.

Step 5 In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



Disabling Auto-Accept Changes for All Devices on the Tenant

Procedure

Step 1 Log-in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 In left pane, click **Administration** > **General Settings**.

Step 3 In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X. This disables Auto-Accept Changes option in the Conflict Detection menu and disables the feature for every device on your tenant.

Note Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into Security Cloud Control. This includes devices previously configured to auto-accept changes.

Resolve Configuration Conflicts

This section provides information about resolving configuration conflicts that occur on the device.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Note For an On-Premises Firewall Management Center, click **Administration** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reported as Not Synced.

Step 5 In the **Not synced** panel to the right, select either of the following:

- **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

Resolve the Conflict Detected Status

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 576 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Note For an On-Premises Firewall Management Center, click **Administration** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.

Step 5 In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

- The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
- The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

Step 6 Resolve the conflict by selecting one of the following:

- **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

  Note As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

Note All configuration changes, rejected or accepted, are recorded in the change log.

Schedule Polling for Device Changes

If you have Conflict Detection, on page 576 enabled, or if you **Enable the option to auto-accept device changes** from the Settings page,Security Cloud Control polls the device for the default interval to determine if a change has been made to the device's configuration outside of Security Cloud Control. You can customize how often Security Cloud Control polls for changes per device. These changes can be applied to more than one device.

If there is no selection configured for a device, the interval is automatically configured for "tenant default".

Note Customizing the interval per device from the **Security Devices** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the Settings page, use the following procedure to schedule how often you want Security Cloud Control to poll your devices:

Procedure

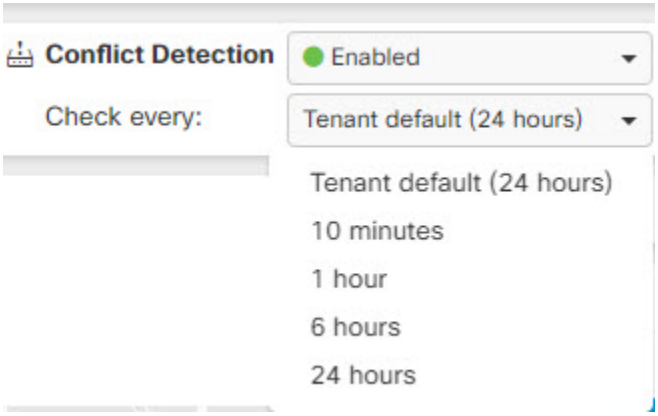
Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the same area as **Conflict Detection**, click the drop-down menu for **Check every** and select the desired polling interval:



Schedule a Security Database Update

This section provides information about scheduling a security database update on the device.

Create a Scheduled Security Database Update

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select a device.

Step 5 In the **Actions** pane, locate the **Security Database Updates** section and click the**add +** button.

Note If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

Step 6 Configure the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 7 Click **Save**.

The device's Configuration Status will change to "Updating Databases".

Edit a Scheduled Security Database Update

Use the following procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select a device.

Step 5 In the **Actions** pane, locate the **Security Database Updates** section and click the edit icon .

Step 6 Edit the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 7 Click **Save**.

Step 8 The device's Configuration Status will change to "Updating Databases".

Update FDM-Managed Device Security Databases

By updating the security databases on an FDM-managed device, you are updating the following: SRUs (intrusion rules), security intelligence (SI), vulnerability databases (VDB), and geolocation databases. If you opt into updating the security databases through the Security Cloud Control UI, note that **all** of the mentioned databases are updated; you cannot select which databases you want to update.

Please note that security database updates cannot be reverted.

Note When you update the security databases, some packets may be dropped or pass uninspected. We recommend you schedule your security database updates during a maintenance window.

Update FDM-Managed Device Security Database While Onboarding

When you onboard an FDM-managed device to Security Cloud Control, part of the onboarding process allows you to **Enable scheduled recurring updates for databases**. This option is checked by default. When enabled, Security Cloud Control immediately checks for and applies any security updates as well as automatically schedules the device to check for additional updates. You are able to modify the date and time of the scheduled task after the device is onboarded.

We recommend enabling the automatic scheduler during the onboarding process to regularly check for and apply security database updates. This way your device will always be up to date. To update the security databases while onboarding your FDM-managed device, see Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key.

Note If you onboard your device with the registration key method, the device must **not** be registered with a smart license. We recommend registering an license. As an alternative method, you can onboard your device using the device's Onboard an FDM-Managed Device Using Username, Password, and IP Address.

Update FDM-Managed Device Security Database After Onboarding

After an FDM-managed device is onboarded to Security Cloud Control, you can configure a device to check for security database updates by scheduling an update. You can modify this scheduled task at any time by selecting the device the update is scheduled for. See Schedule a Security Database Update for more information.

Workflows

Device licenses

Cisco Security Cloud Control cannot update the security databases if there is no license. We recommend that your FDM-managed device has at least an license.

If you are onboarding a device that has no license, this does not inhibit Security Cloud Control from onboarding the device. Instead, the device will experience a **Connectivity** status of "insufficient licenses". To resolve this issue, you must apply the correct licenses through the FDM-managed device UI.

Note If you onboard an FDM-managed device and opt in to schedule future security database updates and the device does **not** have a registered license, Security Cloud Control still creates the scheduled task but does not trigger the task until the appropriate licenses have been applied and the device is successfully synchronized.

Security database updates are pending in FDM

If you update the security databases through the FDM-managed device UI, and you have **conflict detection** enabled on your device, Security Cloud Control detects the pending update as a conflict.

Note If you onboard your FDM-managed device and opt to schedule the updates, Security Cloud Control automatically updates the security databases as well as any other pending changes to the stored configuration during the next deploy. **does not have to be a configuration deploy**

Device has OOB changes, or staged changes, during a security database update

If you schedule a security database update for an FDM-managed device that has out of band (OOB) changes, or staged changes that have not been deployed, Security Cloud Control only checks and updates the security databases. Security Cloud Control does **not** deploy OOB or staged changes.

Device already has a scheduled task to update the security databases

Each device can only have one scheduled task. If the device already has a scheduled task to update the security databases, creating a new one overwrites it. This applies to tasks that are created in either Security Cloud Control or an FDM-managed device.

No security database updates available

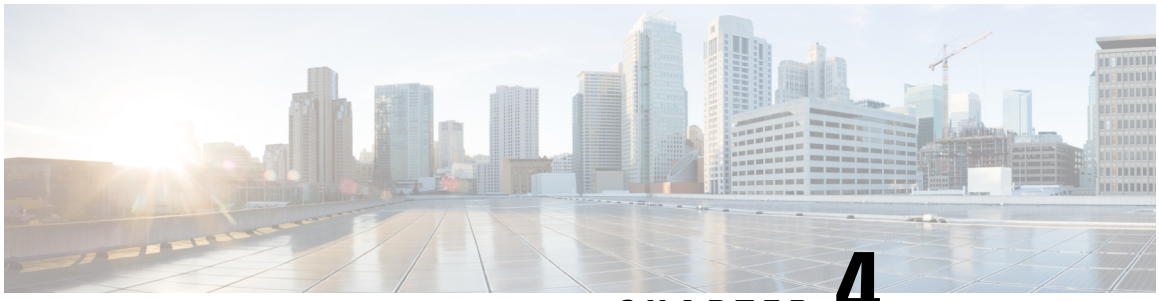
If there are no updates available, Security Cloud Control does not deploy anything to the device.

Security database updates for FDM-managed High Availability (HA) pair

Security database updates are applied only to the primary device of an HA pair.

Related Information:

- Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key
- Onboard an FDM-Managed Device Using Username, Password, and IP Address, on page 166
- Schedule a Security Database Update



CHAPTER 4

Monitoring and Reporting Change Logs, Workflows, and Jobs

Security Cloud Control effectively monitors configuration change logs, bulk device operations, and the process that runs when communicating with devices. This helps you understand how your network's existing policies influence its security posture.

Manage Change Logs in Security Cloud Control

A Change Log captures the configuration changes made in Security Cloud Control, providing a single view that includes changes in all the supported devices and services. These are some of the features of the change log:

- Provides a side-by-side comparison of changes made to device configuration.
- Provides labels for all change log entries.
- Records onboarding and removal of devices.
- Detects policy change conflicts occurring outside Security Cloud Control.
- Provides answers about who, what, and when during an incident investigation or troubleshooting.
- Enables downloading of the complete change log, or only a portion of it, as a CSV file.

Manage Change Log Capacity

Security Cloud Control retains the change log information for one year and deletes data older than a year.

There is a difference between the change log information stored in Security Cloud Control's database and what you see in an exported change log. See Export the Change Log, on page 589 for more information.

Change Log Entries

A change log entry reflects the changes to a single device configuration, an action performed on a device, or the change made to a device outside Security Cloud Control:

- For change log entries that contain configuration changes, you can view details about the change by clicking anywhere in the corresponding row.
- For out-of-band changes made outside Security Cloud Control and are detected as conflicts, the **System User** is reported as the **Last User**.
- Security Cloud Control closes a change log entry after a device's configuration on Security Cloud Control is synced with the configuration on the device, or when a device is removed from Security Cloud Control. Configurations are considered to be in sync after they read the configuration from the device to Security Cloud Control or after deploying the configuration from Security Cloud Control to the device.
- Security Cloud Control creates a new change log entry immediately after completing an existing entry, irrespective of whether the change was a success or failure. Additional configuration changes are added to the new change log entry that opens.
- Events are displayed for read, deploy, and delete actions for a device. These actions close a device's change log.
- A change log is closed after Security Cloud Control is in sync with the configuration on the device (either by reading or deploying), or when Security Cloud Control no longer manages the device.
- If a change is made to the device outside of Security Cloud Control, a *Conflict detected* entry is included in the change log.

Pending and Completed Change Log Entries

Change logs have a status of either Pending or Completed. As you make changes to a device's configuration using Security Cloud Control, these changes are recorded in a Pending change log entry. The following activities complete a Pending change log, and after this a new change log is created for recording future changes.

- Reading a configuration from a device to Security Cloud Control
- Deploying changes from Security Cloud Control to a device
- Deleting a device from Security Cloud Control
- Running a CLI command that updates the running configuration file

Search and Filter Change Log Entries

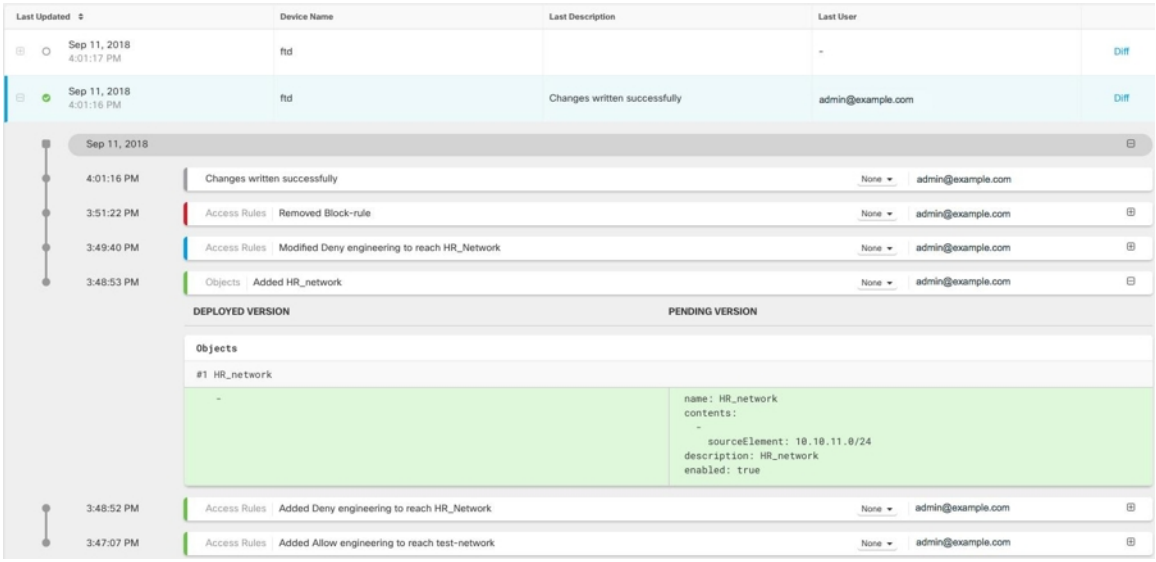
You can search and filter change log entries. Use the search field to find events. Use the filter ( ) to find the entries that meet the criteria you specify. You can also combine the two tasks by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

Change Log Entries After Deploying to FDM-Managed Device

The changes in the change log entries for FDM-managed devices are summarized in simple terms. Clicking a change in the change log entry provides information about the exact changes. After writing changes from Security Cloud Control to your FDM-managed device, the change log entry is moved to **Completed** state and Security Cloud Control creates a new entry for future changes. Clicking the View Change Log Differences link in a change log entry row displays a side-by-side comparison of the changes in the context of the running configuration file.

Each row within a log contains a colored band or outline at the start of the row which indicate the state of the changes. As shown in the image below, red indicates deletions, blue indicates modifications, green indicates additions to the device configuration, and grey indicates messages.

The image below shows the log details for addition of a network object called HR_network. Look at the expanded section for **Added HR_network**. The **Deployed Version** contains information about the configuration present in the device. The **Pending Version** column contains the configuration that are yet to be updated. The **Deployed Version** column is empty because there was no HR_network object on the device before the change. The **Pending Version** column shows that HR_network object was created with the value 10.10.11.0/24.



Change Log Entries After Reading Changes from an FDM-Managed Device

When Security Cloud Control detects a change in an FDM-managed device, it registers a **Conflict Detected** state in the **Inventory** page's **Configuration Status** column. It does not record this status in the change log.

When you accept configuration changes made outside Security Cloud Control, Security Cloud Control creates a job and displays the job's processing status in the lower-right corner of the interface. We recommend that you do not make additional changes until the current job is completed. Doing so might lead to the changes being lost.

After the job successfully completes, click "View Change Log Differences" for the change log entry.

Related Information:

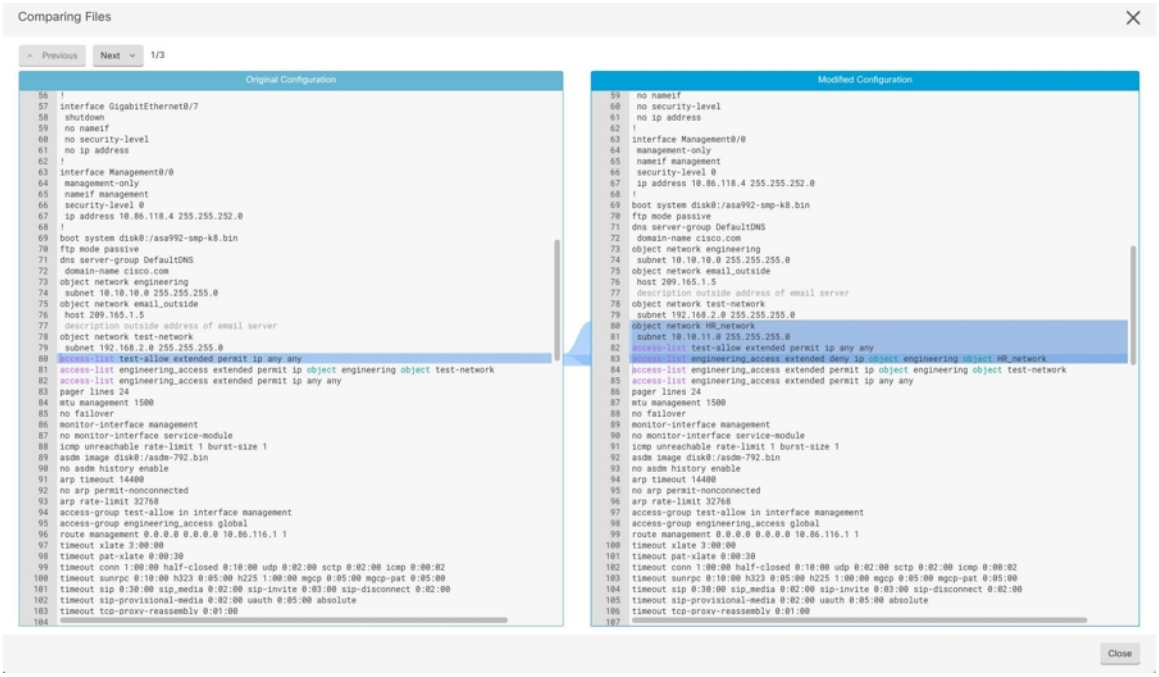
- About Device Configuration Changes, on page 563

View Change Log Differences

Click **Diff** in the change log to open up a side-by-side comparison of the changes in the running configuration file of the device.

In the following figure, the **Original Configuration** column is the running configuration file before a change was written to the ASA. The **Modified Configuration** column shows the running configuration file after the change was written. In this case, the **Original Configuration** column highlights a row in the running configuration file; this row doesn't change, but gives you a point of reference in the **Modified Configuration** column.

Follow the lines across from the left to the right column to see the addition of the *HR_network* object and the access rule preventing addresses in the *engineering* network to reach addresses in the *HR_network* network. Click **Previous** and **Next** to move through the changes in the file.



Related Topics

- Manage Change Logs in Security Cloud Control, on page 585

Export the Change Log

You can export all or a subset of the Security Cloud Control change log to a comma-separated value (.csv) file so that you can filter and sort the information, as required.

To export the change log to a .csv file, follow this procedure:

Procedure

Step 1 In the left pane, click **Events & Logs** > **Change Log**.

Step 2 Find the changes you want to export by doing one of the following tasks:

- Use the filter ( ) and the search field to find what you want to export. For example, filter by device to see only the changes for your selected device or devices.
- Clear all the filters and search criteria in the change log. This allows you to export the entire change log.

Note Security Cloud Control retains 1 year of change log data. It is recommended to filter the change log contents and download the results ot a .csv file rather than downloading the entire change log history for a year.

Step 3 Click the export icon at the top right corner of the page.

Step 4 Save the .csv file to your local file system, with a descriptive name.

Differences Between Change Log Capacity in Security Cloud Control and Size of an Exported Change Log

The information that you export from Security Cloud Control's Change Log page is different from the change log information that Security Cloud Control stores in its database.

For every change log, Security Cloud Control stores two copies of the device's configuration–the *starting* configuration and either the *ending* configuration in the case of a closed change log or the *current* configuration in the case of an open change log. This allows Security Cloud Control to display configuration differences side by side. In addition, Security Cloud Control tracks and stores every step (*change event*) with the username that made the change, the time the change was made, and other details.

However, when you export the change log, the export does not include the two complete copies of the configuration. It only includes the *change events*, which makes the export file much smaller than the change log that Security Cloud Control stores.

Security Cloud Control stores change log information for a year. This includes two copies of the configuration.

Change Request Management

Change Request Management enables the linking of a **Change Request** and its business justification to a **Change Log** event. The **Change Request** is opened in a third-party ticketing system.

Use **Change Request Management** to create a **Change Request** in Security Cloud Control and associate it with change log events. You can search for this change request by **Name** within the change log.

Note In Security Cloud Control, **Change Request Tracking** and **Change Request Management** refer to the same functionality.

Enable Change Request Management

Enabling change request tracking affects all users of your tenant.

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Enable the **Change Request Tracking** toggle button.

When enabled, the **Change Request** menu appears at the bottom-left corner and the **Change Request** drop-down list is available in the **Change Log** page.

Create a Change Request

Procedure

Step 1 In Security Cloud Control, click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Enter a **Name** and **Description**.

Ensure that the **Name** corresponds to a **Change Request** name that your organization intends to use, and that the **Description** describes the purpose of the change.

Note You cannot modify the name of a **Change Request** after you create it.

Step 3 Click **Save**.

Note When a **Change Request** is saved, Security Cloud Control associates all the new changes with the corresponding **Change Request** name. This association continues until you either Disable Change Request Management or Clear the Change Request Toolbar from the menu.

Associate a Change Request with a Change Log Event

Procedure

Step 1 In the left pane, click **Events & Logs** > **Change Log**.

Step 2 Expand the change log to view the events you want to associate with a **Change Request**.

Step 3 Click the drop-down list adjacent to the corresponding change log entry.

Note The latest change requests are displayed at the top of the change request list.

Step 4 Select a change request and click **Select**.

Search for Change Log Events with Change Requests

Procedure

Step 1 In the left pane, click **Events & Logs** > **Change Log**.

Step 2 In the change log search field, enter the name of a change request to find the associated change log events.

Security Cloud Control highlights the change log events that are exact matches.

Search for a Change Request

Procedure

Step 1 In Security Cloud Control, click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Enter the name of the **Change Request** or a relevant keyword in the search field. As you enter a value, the results that partially match your input, appear in both the **Name** and **Description** fields.

Filter Change Requests

Procedure

Step 1 In the left pane, click **Events & Logs** > **Change Log**.

Step 2 Click the filter icon to view all the options.

Step 3 In the search field, enter the name of a **Change Request**.

As you enter a value, the results that partially match your entry appear.

Step 4 Select a change request by checking the corresponding check box.

The matches appear in the **Change Log** table. Security Cloud Control highlights the change log events that are exact matches.

Clear the Change Request Toolbar

To avoid automatic association of change log events with an existing change request, clear the information in the change request toolbar.

Procedure

Step 1 In Security Cloud Control, click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Click **Clear**.

The **Change Request** menu now displays **None**.

Clear a Change Request Associated with a Change Log Event

Procedure

Step 1 In the left pane, click **Events & Logs** > **Change Log**.

Step 2 Expand the **Change Log** to view the events that you want to disassociate from **Change Requests**.

Step 3 Click the drop-down list adjacent to the corresponding change log entry.

Step 4 Click **Clear**.

Delete a Change Request

Deleting a **Change Request** removes it from the change request list, but not from the **Change Log**.

Procedure

Step 1 Click the **Create Change Request** (+) icon in the **Change Request** menu at the bottom-left corner.

Step 2 Select the change request and click the bin icon to delete it.

Step 3 Click the check mark to confirm.

Disable Change Request Management

Disabling **Change Request Management** or **Change Request Tracking** affects all users of your account.

Procedure

Step 1 In the left pane, click **Administration** > **General Settings**.

Step 2 Disable the **Change Request Tracking** toggle button.

Change Request Management Use Cases

These use cases assume that you have enabled Change Request Management.

Track Changes Made to the Firewall Device to Resolve a Ticket Maintained in an External System

This use case describes a scenario where you want to make changes to a firewall device to resolve a ticket maintained in an external system and want to associate the change log events resulting from these firewall changes to a change request. Follow this procedure to create a change request and associate change log events to it:

1. Create a Change Request, on page 590.
2. Use the ticket name or number from the external system as the name of the change request and add the justification for the change and other relevant information in the **Description** field.
3. Ensure that the new change request is visible in the change request toolbar.
4. Make the changes to the firewall device.
5. In the navigation pane, click **Change Log** and find the change log events that are associated with your new change request.
6. Clear the Change Request Toolbar, on page 592 to avoid automatic association of change log events with an existing change request.

Manually Update Individual Change Log Events After Changes are Made to the Firewall Device

This use case describes a scenario where you have made changes to a firewall device to resolve a ticket that is maintained in an external system, but forgot to use the Change Request Management feature to associate change requests with the change log events. You want to update the change log events with the ticket number. Follow this procedure to associate change requests with change log events:

1. Create a Change Request, on page 590. Use the ticket name or number from the external system as the name of the change request. Use the **Description** field to add the justification for the change and other relevant information.
2. In the navigation pane, click **Change Log** and search for the change log events that are associated with the changes.
3. Associate a Change Request with a Change Log Event, on page 591.
4. Clear the Change Request Toolbar, on page 592 to avoid automatic association of change log events with an existing change request.

Search for Change Log Events Associated with a Change Request

This use case describes a scenario where, you want to find out what change log events were recorded in the change log because of the work done to resolve a ticket maintained in an external system. Follow this procedure to search for change log events that are associated with a change request:

1. In the navigation pane, click **Change Log.**
2. Search for change log events that are associated with change requests using one of the following methods below:
   - In the **Change Log** search field, enter the exact name of the change request to find change log events associated with that change request. Security Cloud Control highlights change log events that are exact matches.
   - Filter Change Requests, on page 592 to find the change log events.
3. View each change log to find the highlighted change log events showing the associated change request.

FDM-Managed Device Executive Summary Report

The Executive Summary Report offers a collection of operational statistics for all FDM-managed devices. After a device is onboarded, Security Cloud Control might take up to two hours to collect this information from the Firewall Device Manager. After the initial report generation, data is compiled hourly. Note that report information is not part of the request for events. So events and reports are not available at the same cadence.

Data in the reports is generated when network traffic triggers an access rule or policy on an FDM-managed device. We strongly recommend that you enable malware defense and IPS licenses, as well as file logging for access rules, in order to allow a device to generate the events that are reflected in the reports.

Note that all of the information displayed in the report is dependent on the **Time Range** toggle button located at the top of the page. Policies may experience varying traffic or triggers during the time range you select.

If you experience issues with the Executive Summary Report or see an unexpected amount of traffic, see Troubleshoot the Executive Summary Report, on page 715 for more information.

Generate Network Operation Data

After a device is onboarded to Security Cloud Control, event data is automatically collected. The data that is collected is dependent on the device configuration. The license that is delivered with all FDM-managed devices does not support all the options within the Network Operations Report. We recommend the following configurations for the devices you want to collect data from:

- **Logging** : Enable file logging on applicable access control rules. See Logging Settings in an FDM-Managed Access Control Rule for more information.
- **Malware Events**: Enable the malware Smart License.
- **Security Intelligence**: Enable the Smart License.
- **IPS Threats** : Enable the Smart License.
- **Web Categories** : Enable the URL Smart License.
- **Files Detected**: Enable the Smart License.

See FDM-Managed Device Licensing Types for more information on smart licenses and the capabilities these licenses provide.

Note The executive summary does not inherently include traffic that is flowing over VPN.

Overview

The **Overview** tab displays visuals from triggered rules, threats, and file types. These items are displayed numerically, with the largest or most frequently hit rules, events, or files listed first.

Malware events represent detected or blocked malware files only. Note that the disposition of a file can change, for example, from clean to malware or from malware to clean. We recommend that you Schedule a Security Database Update to keep your devices up to date with the latest intrusion rules (SRUs).

Top Ten Access Rule Hits offers three tabs you can toggle between to view the top ten rule transfers, connections, or rules that blocked packets.

Network Assessment

The **Network Assessment** tab addresses web site categories and detected file types. This display captures only the top ten most frequently encountered categories and file types. Other than selected time range, you cannot use this tab to determine when a specific web category or file type was detected.

Threats

The **Threats** tab displays statistics generated by intrusion events—**Top Attacker** captures the originating IP address of an event, **Top Target** captures the destination IP address of an event, and **Top Threats** captures the type of events that have been categorized as a threat.

This tab also provides details about the threats and malware types that are detected.

Generate a Report

After you configure the report to your preference, generate a PDF of the report. See Generating FDM-Managed Device Executive Summary Reports for more information.

Generating FDM-Managed Device Executive Summary Reports

Security Cloud Control provides several reports that you can use to analyze the impact of your security policies on the traffic going through your FDM-managed devices. An Executive Summary Report summarizes the most impactful malware, threats, and impacted security intelligence. Security Cloud Control polls devices every hour to collect events. To learn more about what the executive summary offers, see FDM-Managed Device Executive Summary Report.

Important The FDM-managed device reports are available only on the FDM-managed device that is currently onboarded to your tenant. These reports are generated hourly and are not part of the request for events. So events and reports are not available at the same cadence. After initially onboarding your FDM-managed device, Security Cloud Control may take up to two hours to generate reports. Until there are reports to display, the **Reports** tab under the **Analytics** option will not be visible.

If you are a About Security Analytics and Logging (SaaS) in Security Cloud Control subscriber, Network Reports do not reflect the events forwarded to the Secure Event Connector (SEC).

Note The data used in traffic-related reports is collected from events triggered by access control rules and other security policies. The generated report does not show traffic for rules in which logging is not enabled, or rules that have not been triggered. Ensure that you configure your rules with the information that matters to you.

The following procedure shows how to generate an Executive Summary Report:

Procedure

Step 1 In the navigation pane, click **Analytics** > **Executive Summary Report**.

Step 2 Select the time range for the reports—**24 Hours**, **7 Dayss**, **30 Days**, or **90 Days**.

Step 3 (Optional) Click the filter ( ) icon to select a custom list of devices, for which to generate a report.

Step 4 Click **Generate Report (PDF)**.

Step 5 To save the report as a PDF, click **Save** and choose **Save as PDF** in the **Destination** drop-down.

Step 6 Browse to the location in which you want to save the report, and click **Save**. If you do not want to save the report, click **Cancel** at any time.

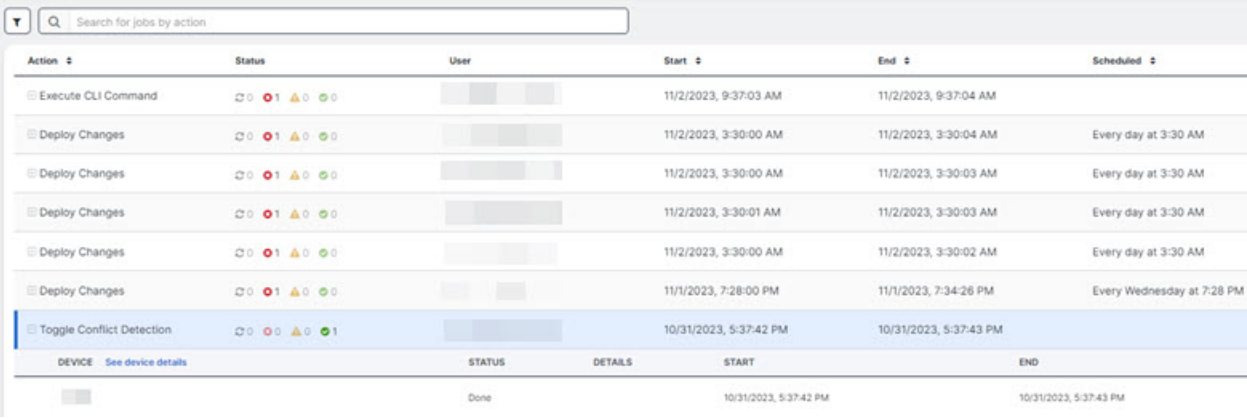
Related Information:

- FDM-Managed Device Executive Summary Report
- Troubleshoot the Executive Summary Report, on page 715

Monitor Jobs in Security Cloud Control

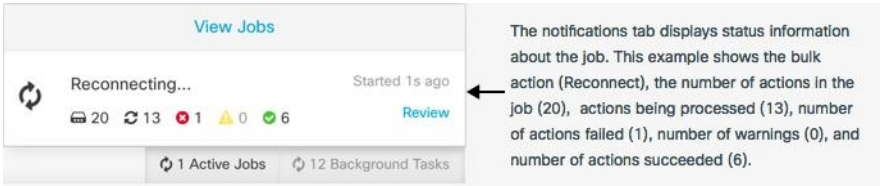
The **Jobs** page provides an overview of the progress of bulk operations, such as reconnecting multiple devices, reading configurations from multiple devices, or upgrading multiple devices simultaneously. The **Jobs** table uses color-coded rows along with the status of individual actions, indicating if they have succeeded or failed.

One row in the table represents a single bulk operation. This one bulk operation may have been, for example, an attempt to reconnect 20 devices. Expanding a row in the **Jobs** page displays the results for each of the devices affected by the bulk operation.



You can reach the **Jobs** page in two different ways:

- In the **Notifications** tab, when there is a new Job notification, click the **Review** link. You will be redirected to the **Jobs** page and see the specific job represented by the notification.



- In the left pane, click **Events & Logs** > **Jobs**. This table shows a complete list of the bulk actions performed in Security Cloud Control.

Search Jobs in Security Cloud Control

When you're on the **Jobs** page, you can filter and search by different actions, the users who performed them, and the action status.

Reinitiate a Bulk Action

After reviewing the **Jobs** page, if you find that one or more actions in a bulk action have failed, you can retry the bulk action after making the necessary corrections.. Note that Security Cloud Control will re-run the job only for the failed actions. To re-run a bulk action:

Procedure

Step 1 In the **Jobs** page. select the row that indicates a failed action.

Step 2 Click the **Retry**( ) icon.

Cancel a Bulk Action

You can cancel the bulk actions that are currently in progress on multiple devices. For example, if you have tried to reconnect four managed devices, and three of them have successfully reconnected, but the fourth device is still neither connected nor disconnected, you can cancel the bulk action.

To cancel a bulk action:

Procedure

Step 1 In the left pane, click **Events & Logs** > **Jobs**.

Step 2 Identify the running bulk action and click the **Cancel** link on the right side.

Note If any part of the bulk action is successful, it cannot be undone. Any ongoing action will be cancelled.

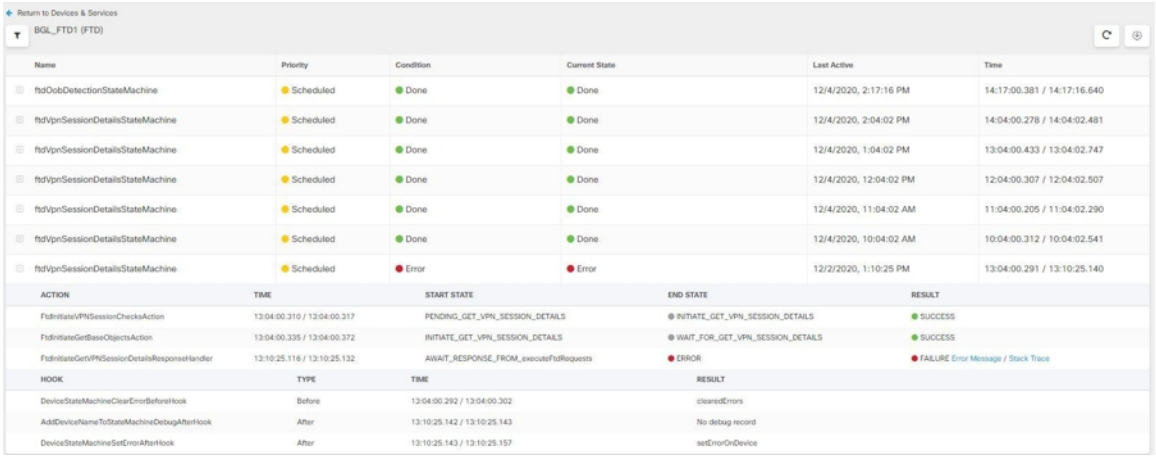
Monitor Workflows in Security Cloud Control

The **Workflows** page allows you to monitor every process that Security Cloud Control runs when communicating with devices, Secure Device Connector (SDC), or Secure Event Connector (SEC), and when applying ruleset changes to devices. Security Cloud Control creates an entry in the workflow table for every step and displays its outcome on this page. The entry contains information pertaining only to the action performed by Security Cloud Control and not the device it is interacting with.

Security Cloud Control reports an error when it fails to perform a task on a device. Navigate to the **Workflows** page to see the step where the error occurred, for more details.

This page also helps you determine and troubleshoot errors or share information with TAC, when required.

To navigate to the **Workflows** page, in the left pane, click **Security Devices** and, click the **Devices** tab. Click the appropriate device type tab to locate the device and select the device you want. Under the **Devices and Actions** in the right pane, click **Workflows**. This figure shows the **Workflows** page with entries in the **Workflow** table.

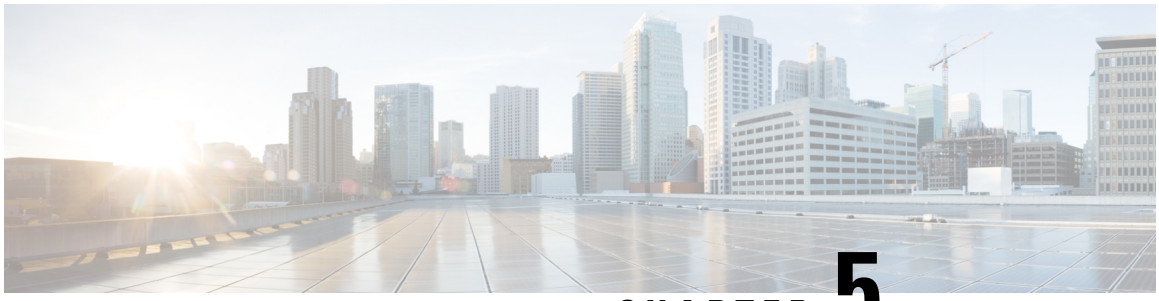


Export Device Workflows

You can download the complete workflow information to a JSON file and provide it when the TAC team asks for further analysis. To export the workflow information, select the corresponding device and, navigate to its **Workflows** page and click the export ( ) icon appearing at the top-right corner.

Copy Stack Trace

If you have an error you cannot resolve and you approach TAC, they may ask you for a copy of the stack trace. To collect the stack trace for the error, click the **Stack Trace** link and click **Copy Stacktrace** to copy the stacks appearing on the screen, to a clipboard.



CHAPTER 5

Cisco Security Analytics and Logging

About Security Analytics and Logging (SaaS) in Security Cloud Control

Cisco Security Analytics and Logging (SAL) allows you to capture connection, intrusion, file, malware, security intelligence, syslog, and Netflow Secure Event Logging (NSEL) events from all of your ASA and Secure Firewall Threat Defense devices and view them in one place in Security Cloud Control. The events are stored in the Cisco cloud and viewable from the **Event Logging** page in Security Cloud Control, where you can filter and review them to gain a clear understanding of what security rules are triggering in your network.

With additional licensing, after you capture these events, you can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal provisioned for you. Secure Cloud Analytics is a software as a service (SaaS) solution that tracks the state of your network by performing a behavioral analysis on events and network flow data. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Terminology Note: In this documentation, when Cisco Security Analytics and Logging is used with the Secure Cloud Analytics portal (a software as a service product) you will see this integration referred to as Cisco Security Analytics and Logging (SaaS) or SAL (SaaS).

Event Types in Security Cloud Control

When filtering ASA and Secure Firewall Threat Defense events logged by Secure Logging Analytics (SaaS), you can choose from a list of ASA and FTD event types that Security Cloud Control supports. From the Security Cloud Control menu, navigate **Analytics** > **Event Logging** and click the filter icon to choose events. These event types represent groups of syslog IDs. The table that follows shows which syslog IDs are included in which event type. If you want to learn more about a specific syslog ID, you can search for it in the Cisco ASA Series Syslog Messages or the Cisco Secure Firewall Threat Defense Syslog Messages guides.

Some syslog events have the additional attribute "EventName." You can filter the events table to find events using the EventName attribute by filtering by attribute:value pairs. See EventName Attributes for Syslog Events.

Some syslog events will have the additional attributes "EventGroup" and "EventGroupDefinition". You will be able to filter the events table to find events using these additional attributes by filtering by attribute:value pairs. See EventGroup and EventGroupDefinition Attributes for Some Syslog Messages.

The NetFlow events are different from syslog events. The **NetFlow** filter searches for all NetFlow event IDs that resulted in an NSEL record. Those NetFlow event IDs are defined in the Cisco ASA NetFlow Implementation Guide.

The following table describes the event types that Security Cloud Control supports and lists the syslog or NetFlow event numbers that correspond to the event types:

Filter Name	Description	Corresponding Syslog Event or Netflow Event
AAA	These are events that the system generates when failed or invalid attempts happen to authenticate, authorize, or use up resources in the network, when AAA is configured.	109001-109035 113001-113027
BotNet	These events get logged when a user attempts to access a malicious network, which might contain a malware-infected host, possibly a BotNet, or when the system detects traffic to or from a domain or an IP address in the dynamic filter block list.	338001-338310
Failover	These events get logged when the system detects errors in stateful and stateless failover configurations or errors in the secondary firewall unit when a failover occurs.	101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	These events get generated when the firewall system denies traffic of a network packet for various reasons, ranging from a packet drop because of the security policy to a drop because the system received a packet with the same source IP and destination IP, which could potentially mean an attack on the network. Firewall Denied events may be contained in a NetFlow and may be reported with NetFlow event IDs as well as syslog IDs.	106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Firewall Traffic	These are events that get logged depending on the various connection attempts in the network, user identities, time stamps, terminated sessions, and so on. Firewall Traffic events may be contained in a NetFlow and may be reported with NetFlow event IDs as well as syslog IDs.	106001-106100, 108001-108007, 110002-110003 201002-201013, 209003-209005, 215001 302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009 400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001 500001-500005, 508001-508002 607001-607003, 608001-608005, 609001-609002, 616001 703001-703003, 726001
IPsec VPN	These events are logged in an IPsec VPN-configured firewall when mismatches occur in IPsec security associations or when the system detects an error in the IPsec packets it receives.	402001-402148, 602102-602305, 702304-702307
NAT	These events are logged in a NAT-configured firewall when NAT entries are created or deleted and when all the addresses in a NAT pool are used up and exhausted.	201002-201013, 202001-202011, 305005-305012
SSL VPN	These events are logged in an SSL VPN-configurated firewall when WebVPN sessions get created or terminated, user access errors, and user activities.	716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015
NetFlow	These events are logged around the IP network traffic as network packets enter and exit the interfaces, timestamps, user identities, and the amount of data transferred.	0, 1, 2, 3, 5

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Connection	You can generate events for connections as users generate traffic that passes through the system. Enable connection logging on access rules to generate these events. You can also enable logging on Security Intelligence policies and SSL decryption rules to generate connection events. Connection events contain data about the detected sessions. The information available for any individual connection event depends on several factors, but in general includes: • Basic connection properties: timestamp, source and destination IP address, ingress and egress zones, the device that handled the connection, and so on. • Additional connection properties discovered or inferred by the system: applications, requested URLs, or users associated with the connection, and so on. • Metadata about why the connection was logged: which configuration handled the traffic, whether the connection was allowed or blocked, details about encrypted and decrypted connections, and so on.	430002, 430003

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Intrusion	The system examines the packets that traverse your network for malicious activity that could affect the availability, integrity, and confidentiality of a host and its data. When the system identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, type of exploit, and contextual information about the source of the attack and its target. Intrusion events are generated for any intrusion rule set to block or alert, regardless of the logging configuration of the invoking access control rule.	430001
File	File events represent files that the system detected, and optionally blocked, in network traffic based on your file policies. You must enable file logging on the access rule that applies the file policy to generate these events. When the system generates a file event, the system also logs the end of the associated connection regardless of the logging configuration of the invoking access control rule.	430004

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Malware	The system can detect malware in network traffic as part of your overall access control configuration. AMP for Firepower can generate a malware event, containing the disposition of the resulting event, and contextual data about how, where, and when the malware was detected. You must enable file logging on the access rule that applies the file policy to generate these events. The disposition of a file can change, for example, from clean to malware or from malware to clean. If AMP for Firepower queries the AMP cloud about a file, and the cloud determines the disposition has changed within a week of the query, the system generates retrospective malware events.	430005
Security Intelligence	Security Intelligence events are a type of connection event generated by the Security Intelligence policy for each connection that is blocked or monitored by the policy. All Security Intelligence events have a populated Security Intelligence Category field. For each of these events, there is a corresponding "regular" connection event. Because the Security Intelligence policy is evaluated before many other security policies, including access control, when a connection is blocked by Security Intelligence, the resulting event does not contain the information that the system would have gathered from subsequent evaluation, for example, user identity.	430002, 430003

Secure Logging Analytics for FDM-Managed Devices

Cisco Security Analytics and Logging (SaaS) allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your FDM-managed devices and view them in one place in Security Cloud Control.

The events are stored in the Cisco cloud and viewable from the Event Logging page in Security Cloud Control where you can filter and review them to gain a clear understanding of what security rules are triggering in your network. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Logging Analytics and Detection** package (formerly **Firewall Analytics and Logging** package), the system can apply Secure Cloud Analytics dynamic entity modeling to your FDM-managed device events, and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your FDM-managed device events and your network traffic, and generates observations and alerts. You can cross-launch from Security Cloud Control to a Cisco Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

How FDM Events are Displayed in the Security Cloud Control Events Viewer

Connection, intrusion, file, malware, and Security Intelligence events are generated when an individual rule is configured to log events and network traffic matches the rule criteria. After the events are stored in the Cisco cloud, you can view them in Security Cloud Control. There are two methods of configuring your FDM-managed device to send events to the Cisco cloud:

- You can install multiple Secure Event Connectors (SECs) and send events generated by a rule, on any device, to any of the SECs as if it were a syslog server. The SEC then forwards the event to the Cisco cloud.
- If your FDM-managed device was onboarded to Security Cloud Control using a registration key, you can send events directly to the Cisco cloud using a control in the Secure Firewall device manager.

How an Event is Sent to the Cisco Cloud Using the Secure Event Connector

With the basic **Logging and Troubleshooting** license, this is how a Secure Firewall device manager event reaches the Cisco cloud:

1. You onboard your FDM-managed device to Security Cloud Control using username and password or by using a registration key.
2. You configure individual rules, such as access control rules, Security Intelligence rules, and SSL decryption rules, to forward events to any one of your SECs as if it were a syslog server. In access control rules, you can also enable file and malware policies, and intrusion policies, and forward events generated by those polices to the SEC.
3. You configure File/Malware logging in **System Settings** > **Logging** for file events.
4. You configure Intrusion Logging in **System Settings** > **Logging** for intrusion events.
5. The SEC forwards the events to the Cisco cloud where the events are stored.
6. Security Cloud Control displays events from the Cisco cloud in its Events Logging page based on the filters you set.

With the **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, the following also occur:

1. Cisco Secure Cloud Analytics applies analytics to the Secure Firewall device manager connection events stored in the Cisco cloud.
2. Generated observations and alerts are accessible from the Secure Cloud Analytics portal associated with your Security Cloud Control portal.
3. From the Security Cloud Control portal, you can cross-launch your Secure Cloud Analytics portal to review these observations and alerts.

How Events are Sent Directly from an Secure Firewall device manager to the Cisco Cloud

With the basic **Logging and Troubleshooting license**, this is how Secure Firewall device manager events reach the Cisco cloud:

1. You onboard your FDM-managed device to Security Cloud Control using a registration token.
2. You configure individual rules, such as access control rules, Security Intelligence rules, and SSL decryption rules, to log events but you don't specify a syslog server for them to be sent to. In access control rules, you can also enable file and malware policies and intrusion policies, and forward events generated by those polices to the Cisco cloud.
3. File events and Intrusion events are sent to the Cisco cloud if file and malware policies and intrusion policies are configured in the access control rules to log connection events.
4. You activate Cloud Logging on the Secure Firewall device manager and the events logged in the various rules are sent to the Cisco cloud.
5. Security Cloud Control pulls events from the Cisco cloud based on the filters you set and displays them in its Events viewer.

With the **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, the following also occur:

1. Cisco Secure Cloud Analytics applies analytics to the Secure Firewall device manager connection events stored in the Cisco cloud.
2. Generated observations and alerts are accessible from the Secure Cloud Analytics portal associated with your Security Cloud Control portal.
3. From the Security Cloud Control portal, you can cross-launch your Secure Cloud Analytics portal to review these observations and alerts.

Configuration Comparison

Here is a summary of the Security Cloud Control configuration differences between sending events to the Cisco cloud through an SEC and sending events directly to the Cisco cloud.

FDM-Managed Device Configuration	When Sending Events through a Secure Event Connector (SEC)	When Sending Events Directly to Cisco Cloud
Security Cloud Control onboarding method for FDM-Managed Device	Credentials (Username and password) Registration token	Registration token Serial Number
Version Support	Version 6.4+	Registration Token - Version 6.5+ Serial Number - Version 6.7+
Cisco Security Analytics and Logging (SaaS) Licenses	Logging and Troubleshooting Logging Analytics and Detection (optional) Total Network Analytics and Monitoring (optional)	Logging and Troubleshooting Logging Analytics and Detection (optional) Total Network Analytics and Monitoring (optional)
Licenses	license -If you want to collect connection events from intrusion rules, file control rules, or security intelligence filtering. Malware-If you want to collect connection events from file control rules.	license -If you want to collect connection events from intrusion rules, file control rules, or security intelligence filtering. Malware-If you want to collect connection events from file control rules.
Secure Event Connector	Required	N/A
Data Compression*	Events are compressed*	Events are not compressed*
Data Plan	Required	Required

Note Data subscriptions and your Historical Monthly Usage are based on the amount uncompressed data you use.

Components in the Solution

Cisco Security Analytics and Logging (SaaS) uses these components to deliver events to Security Cloud Control:

Secure Device Connector (SDC)-The SDC connects Security Cloud Control to your FDM-managed devices. The login credentials for the FDM-managed devices are stored on the SDC. See Secure Device Connector, on page 14 for more information.

Secure Event Connector (SEC)-The SEC is an application that receives events from your FDM-managed devices and forwards them to the Cisco cloud. Once in the Cisco cloud, you can view the events on Security Cloud Control's Event Logging page or analyze them with Cisco Secure Cloud Analytics. You may have one or more SECs associated with your tenant. Depending on your environment, you install the Secure Event Connector on a Secure Device Connector or a Security Cloud Control Connector VM.

Secure Firewall device manager-The FDM-managed device is Cisco's next generation firewall. Beyond stateful inspection of network traffic and access control, the FDM-managed device provides capabilities such as protection from malware and application-layer attacks, integrated intrusion prevention, and cloud-delivered threat intelligence.

If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, Cisco Security Analytics and Logging (SaaS) uses Cisco Secure Cloud Analytics to further analyze events delivered to Security Cloud Control.

Cisco Secure Cloud Analytics-Secure Cloud Analytics applies dynamic entity modeling to events, generating detections based on this information. This provides a deeper analysis of telemetry gathered from your network, allowing you to identify trends and examine anomalous behavior in your network traffic.

Licensing

To configure this solution you need the following accounts and licenses:

Security Cloud Control. You must have a Security Cloud Control tenant.

Secure Device Connector. There is no separate license for a SDC.

Secure Event Connector. There is no separate license for a SEC.

Secure Logging Analytics (SaaS). You need to buy the **Logging and Troubleshooting** license. The goal of this package is to provide network operations teams with real-time and historical events derived from their on-boarded FDM-managed devices for the purposes of troubleshooting and analyzing traffic in their network.

You can also buy a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license to apply Cisco Secure Cloud Analytics. The goal of these packages is to provide network operations teams additional insight into the events (and network traffic with the Total Network Analytics and Monitoring license) to better identify possible anomalous behavior and respond to it.

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Logging and Troubleshooting	View events and event detail within Security Cloud Control, both as a live feed and as a historical view	• 1 year • 3 years • 5 years	• Security Cloud Control • An on-premises deployment running version 6.4 or later . • Deployment of one or more SECs to pass events to the cloud

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Logging Analytics and Detection (formerly **Firewall Analytics and Monitoring**)	**Logging and Troubleshooting** functionality, plus: • Apply dynamic entity modeling and behavioral analytics to your FDM-managed device events • Open alerts in Secure Cloud Analytics based on event data, cross-launching from the Security Cloud Control event viewer	• 1 year • 3 years • 5 years	• Security Cloud Control • An on-premises deployment running version 6.4 or later. • Deployment of one or more SECs to pass events to the cloud. • A newly provisioned or existing Secure Cloud Analytics portal.
Total Network Analytics and Monitoring	**Logging Analytics and Detection**, plus: • Apply dynamic entity modeling and behavioral analytics to events, on-premises network traffic, and cloud-based network traffic. • Open alerts in Secure Cloud Analytics based on the combination of event data, on-premises network traffic flow data collected by Secure Cloud Analytics sensors, and cloud-based network traffic passed to Secure Cloud Analytics, cross-launching from the Security Cloud Control event viewer.	• 1 year • 3 years • 5 years	• Security Cloud Control • An on-premises deployment running version 6.4 or later . • Deployment of one or more SECs to pass events to the cloud . • Deployment of at least one Secure Cloud Analytics sensor version 4.1 or later to pass network traffic flow data to the cloud OR integrating Secure Cloud Analytics with a cloud-based deployment, to pass network traffic flow data to Secure Cloud Analytics. • A newly provisioned or existing Secure Cloud Analytics portal.

FDM-Managed Device. You need to have the following licenses to run the FDM-managed device and create rules that generate security events:

License	Duration	Granted Capabilities
Essentials(automatically included)	Perpetual	All features not covered by the optional term licenses. You must also specify whether to **Allow export-controlled functionality on the products registered with this token**. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.
	Term-based	**Intrusion detection and prevention**-Intrusion policies analyze network traffic for intrusions and exploits and, optionally, drop offending packets. **File control**-File policies detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types. AMP for Firepower, which requires a Malware license, allows you to inspect and block files that contain malware. You must have the Threat license to use any type of File policy. **Security Intelligence filtering**-Drop selected traffic before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to immediately drop connections based on the latest intelligence.
Malware	Term-based	File policies that check for malware, which use Cisco Advanced Malware Protection (AMP) with AMP for Firepower (network-based Advanced Malware Protection) and Cisco Threat Grid. File policies can detect and block malware in files transmitted over your network.

Data Plans

You need to buy a data storage plan that reflects the number of events the Cisco cloud receives from your on-boarded FDM-managed devices on a daily basis. The best way to determine your ingest rate is to participate in a free trial of Secure Logging Analytics (SaaS) (SaaS) before you buy it. This will give you a good estimate of your event volume. In addition, you can use the Logging Volume Estimator Tool.

Caution It is possible to configure your FDM-managed device to send events to the Cisco cloud directly and by way of the SEC simultaneously. If you do this, the same event will be "ingested" twice and counted against your data plan twice, though it will only be stored in the Cisco cloud once. Be careful to send events to the Cisco cloud using one method or the other to avoid incurring unnecessary fees.

Data plans are available in 1 GB daily volumes increments, and in 1, 3 or 5 year terms. See the Secure Logging Analytics (SaaS) Ordering Guide for information about data plans.

Note If you have a Security Analytics and Logging license and data plan, then obtain a different license at a later date, that alone does not require you to obtain a different data plan. If your network traffic throughput changes and you obtain a different data plan, that alone does not require you to obtain a different Security Analytics and Logging license.

30-day Free Trial

You can request a 30-day risk-free trial by logging in to Security Cloud Control and navigating to **Events & Logs** > **Events**. On completion of the 30-day trial, you can order the desired event data volume to continue the service from Cisco Commerce Workspace (CCW), by following the instructions in the Secure Logging Analytics (SaaS) ordering guide.

What to do next?

Continue with Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices, on page 614.

Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices

Before you Begin

- Review Secure Logging Analytics for FDM-Managed Devices, on page 608 to learn about:
  - How events are sent to the Cisco cloud
  - Applications in the solution
  - Licenses you need
  - Data plan you need

- You have contacted your managed service provider or Security Cloud Control Sales representative and you have a Security Cloud Control tenant.
- Your tenant may or may not use an Secure Device Connector (SDC) for Security Cloud Control to connect with your FDM-managed devices. Your tenant should have an SDC installed for those FDM-managed devices that you onboard with device credentials, Secure Device Connector. If you onboard your FDM-managed devices with registration key or serial number you do not need an SDC.
- If you have installed an SDC for your tenant, ensure your SDC status is **Active** and has recorded a recent heartbeat.
- If you are installing an SDC, you use one of these methods for the installation:
  - Use Deploy a Secure Device Connector Using Security Cloud Control's VM Image to install an SDC using Security Cloud Control's prepared VM image. This is the preferred and easiest way to deploy an SDC.
  - Use Deploy a Secure Device Connector On Your VM.
- You can Installing an SEC Using a Security Cloud Control Image SEC for your tenant and you can send events from any Firewall device manager to any one SEC onboarded to your tenant.
- If you are sending events directly to the Cisco cloud from the firewall device manager, you have opened up outbound access on port 443 on the management interface.
- You have Sign in to Security Cloud Control for users of your account.

New Security Cloud Control Customer Workflow to Implement Secure Logging Analytics (Saas) and Send Events through the Secure Event Connector to the Cisco Cloud

1. Onboard a Threat Defense Device. You can onboard the device with the admin username and password or with a registration token.
2. Syslog Server Objects.
3. FDM-Managed Access Control Policy to log connection events.
4. Configure your FDM-managed device to Send FDM Events to Security Cloud Control Events Logging.
5. Confirm events are visible in Security Cloud Control. From the navigation bar, select **Events & Logs** > **Events**. Click the Live tab to view live events.
6. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with Analyzing Events in Cisco Secure Cloud Analytics.

New Security Cloud Control Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events Directly to the Cisco Cloud

1. Onboard a Threat Defense Device. You can only use a registration key.
2. FDM-Managed Access Control Policy to log connection events.
3. Configure your FDM-managed device to Send FDM-Managed Events Directly to the Cisco Cloud.
4. Confirm events are visible in Security Cloud Control. From the navigation bar, select **Events & Logs** > **Events**. Click the Live tab to view live events.

5. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with Analyzing Events in Cisco Secure Cloud Analytics.

Existing Security Cloud Control Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud

1. Onboard a Threat Defense Device. You can onboard the device with the admin username and password or with a registration token.
2. Syslog Server Objects.
3. FDM-Managed Access Control Policy to log connection events.
4. Send FDM Events to Security Cloud Control Events Logging.
5. Confirm events are visible in Security Cloud Control. From the navigation bar, select **Events & Logs** > **Events**. Click the Live tab to view live events.
6. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with Analyzing Events in Cisco Secure Cloud Analytics.

Existing Security Cloud Control Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events Directly to the Cisco Cloud

1. Onboard a Threat Defense Device. You can only use a registration key.
2. FDM-Managed Access Control Policy to log connection events.
3. Configure your FDM-managed device to Send FDM-Managed Events Directly to the Cisco Cloud.
4. Confirm events are visible in Security Cloud Control. From the navigation bar, select **Events & Logs** > **Events**. Click the Live tab to view live events.
5. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with Analyzing Events in Cisco Secure Cloud Analytics.

Analyzing Events in Cisco Secure Cloud Analytics

If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, perform the following in addition to the previous steps:

1. Provision a Cisco Secure Cloud Analytics Portal, on page 648.
2. Deploy one or more Secure Cloud Analytics sensors to your internal network if you purchased a **Total Network and Monitoring** license. See Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting, on page 650.
3. Invite users to create Secure Cloud Analytics user accounts, tied to their Cisco Single Sign-On credentials. See Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control, on page 651.
4. Cross-launch from Security Cloud Control to Secure Cloud Analytics to monitor the Secure Cloud Analytics alerts generated from firewall device manager events. See Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control, on page 651.

Reviewing Secure Cloud Analytics Alerts by Cross-launching from Security Cloud Control

With a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, you can cross-launch from Security Cloud Control to Secure Cloud Analytics to review the alerts generated by Secure Cloud Analytics, based on firewall device manager events.

Review these articles for more information:

- Sign in to Security Cloud Control
- Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control, on page 651
- Cisco Secure Cloud Analytics and Dynamic Entity Modeling, on page 652
- Working with Alerts Based on Firewall Events

Secure Analytics and Logging (SaaS) Workflows

Troubleshooting Network Problems Using Security and Analytics Logging Events describes using the events generated from Secure Logging Analytics (SaaS) to determine why a user can't access a network resource.

See also Working with Alerts Based on Firewall Events.

Send FDM Events to Security Cloud Control Events Logging

To view FDM-managed events from access control rules, security intelligence rules, and SSL decryption rules in the Event Logging viewer, you first need to send those events to the Cisco cloud.

- **Access Control Rules**. You can log Event Types in Security Cloud Control at the beginning or end of a network connection. See Configure the FDM Access Control Policy and Logging Settings in an FDM-Managed Access Control Rule for more information about configuring logging for this rule type.
- **Security Intelligence Rules**. You can log Event Types in Security Cloud Control generated by the Security Intelligence rules. If you enable logging, any matches to blocked list entries are logged. Matches to exception entries are not logged, although you get log messages if exempted connections match access control rules with logging enabled. See Configure Firepower Security Intelligence Policy for more information about configuring logging.
- **SSL Decryption Rules**. You can log Event Types in Security Cloud Control generated by SSL decryption rules.

If you are sending file and malware events or intrusion events events to the Cisco cloud and you are using a Secure Event Connector, you need to Configure Logging Settings.

Related Information:

- Create a Syslog Server Object for Secure Logging Analytics (SaaS)

Send FDM-Managed Events Directly to the Cisco Cloud

Starting with Firewall device manager Version 6.5, you can send connection events, intrusion, file, and malware events directly from your FDM-managed device to the Cisco cloud. Once in the Cisco cloud, you can monitor them with Security Cloud Control and analyze them with Cisco Secure Cloud Analytis. This method does not

require installing a Secure Event Connector (SEC) container on the Secure Device Connector (SDC) virtual machine.

Before you begin

Review these topics:

- Secure Logging Analytics for FDM-Managed Devices, on page 608
- Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices

Procedure

Step 1 Log on to the Firewall device manager for the device from which you want to send events to the Cisco cloud.

Step 2 Select **Device** > **System Settings** > **Cloud Services**.

Step 3 In the Send Events to the Cisco Cloud pane, click **Enable**.

Implementing SAL (SaaS) for Cloud-Delivered Firewall Management Center-Managed Devices

To deploy this integration, you must set up event data storage in SAL (SaaS) using either syslog or a direct connection.

- Send Cloud-delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog, on page 622
- Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection, on page 624

Requirements, Guideline, and Limitations for the SAL (SaaS) Integration

Type	Description
Cisco Secure Firewall Threat Defense	• Security Cloud Control-managed standalone threat defense devices, Version, 7.2 and later. • To send events using syslog, you must have threat defense device version 6.4 or later. • To send events directly, you must have threat defense device version 7.2 or later. • To optionally exclude threat defense devices from sending events directly, you must have threat defense device version 7.4.1 or later. • Your firewall system must be deployed and successfully generating events.
Regional cloud	• Determine the regional cloud that you want to send events to. • Events cannot be viewed from or moved between different regional clouds. • If you use a direct connection to send events to the Cisco Security Cloud for integration with Cisco SecureX, or Cisco SecureX threat response, or Cisco XDR, you must use the same cloud region for this integration. • If you send events directly, the regional cloud you specify in Security Cloud Control must match the region of your Security Cloud Control tenant.
Data plan	• You must buy a data plan that reflects the number of events the Cisco cloud receives from your threat defense devices daily. This is called your daily ingest rate. • Use the Logging Volume Estimator Tool to estimate your data storage requirements.
Accounts	When you purchase a license for this integration, you are provided with a Security Cloud Control tenant account to support the integration.

Type	Description
Connectivity	

Type	Description
	The threat defense devices must be able to connect outbound on port 443 to the Cisco Security Cloud at the following addresses: • US region: • api-sse.cisco.com • mx*.sse.itd.cisco.com • dex.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • registration.us.sse.itd.cisco.com • us.manage.security.cisco.com • edge.us.cdo.cisco.com • EU region: • api.eu.sse.itd.cisco.com • mx*.eu.sse.itd.cisco.com • dex.eu.sse.itd.cisco.com • eventing-ingest.eu.sse.itd.cisco.com • registration.eu.sse.itd.cisco.com • eu.manage.security.cisco.com • edge.eu.cdo.cisco.com • Asia (APJ) region: • api.apj.sse.itd.cisco.com • mx*.apj.sse.itd.cisco.com • dex.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com • registration.apj.sse.itd.cisco.com • apj.cdo.cisco.com • edge.apj.cdo.cisco.com • Australia region: • api.aus.sse.itd.cisco.com • mx*.aus.sse.itd.cisco.com • dex.au.sse.itd.cisco.com

Type	Description
	• eventing-ingest.aus.sse.itd.cisco.com • registration.au.sse.itd.cisco.com • aus.cdo.cisco.com • India region: • api.in.sse.itd.cisco.com • mx*.in.sse.itd.cisco.com • dex.in.sse.itd.cisco.com • eventing-ingest.in.sse.itd.cisco.com • registration.in.sse.itd.cisco.com • in.cdo.cisco.com

Send Cloud-delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog

This procedure provides information about the configuration for sending syslog messages for security events (connection, security intelligence, intrusion, file, and malware events) from devices managed by Security Cloud Control.

Before you begin

- Configure policies to generate security events, and verify that the events you expect to see are displayed in the applicable tables under the **Events & Logs** menu.
- Gather information relating to the syslog server IP address, port, and protocol (UDP or TCP).
- Ensure that your devices can reach the syslog server.

Procedure

Step 1 In the left pane, click **Administration** > **Integrations & Migration** > **Cloud Services** to open the **Services** page.

Step 2 Click and select **Cloud-Delivered FMC** and then click **Configuration**.

Step 3 Configure the syslog settings for your threat defense device:

a) Click **Devices** > **Platform Settings** and edit the platform settings policy that is associated with your threat defense device.

b) In the left-side navigation pane, click **Syslog** and configure the syslog settings as follows:

Click this UI Element...	To Do the Following:
Logging Setup	Enable logging, specify FTP server settings, and the Flash usage.
Logging Destination	Enable logging to specific destinations and to specify filtering by message severity level, event class, or by a custom event list.
E-mail Setup	Specify the email address that is used as the source address for syslog messages that are sent as emails.
Events Lists	Define a custom event list that includes an event class, a severity level, and an event ID.
Rate Limit	Specify the volume of messages being sent to all the configured destinations and define the message severity level to which you want to assign the rate limits.
Syslog Settings	Specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination.
Syslog Servers	Specify the IP address, protocol that is used, format, and security zone for the syslog server that is designated as a logging destination.

c) Click **Save**.

Step 4 Configure the general logging settings for the access control policy (including file and malware logging):

a) Click **Policies** > **Access Control** and then edit the access control policy that is associated with your threat defense device.

b) Click **More** and then choose **Logging**. Configure the general logging settings for the access control policy (including file and malware logging) as follows:

Click this UI Element...	To Do the Following:
Send using specific syslog alert	Select a syslog alert from the list of existing predefined alerts or add one by specifying the name, logging host, port, facility, and severity.
Use the syslog settings configured in the FTD Platform Settings policy deployed on the device	Unify the syslog configuration by configuring it in **Platform Settings** and reuse the settings in the access control policy. The selected severity is applied to all the connection and intrusion events. The default severity is **ALERT**.
Send Syslog messages for IPS events	Send events as syslog messages. The default syslog settings are used unless you override them.

Click this UI Element...	To Do the Following:
Send Syslog messages for File and Malware events	Send file and malware events as syslog messages. The default syslog settings are used unless you override them.

c) Click **Save**.

Step 5 Enable logging for security intelligence events for the access control policy:

a) In the same access control policy, click the **Security Intelligence** tab.

b) Click the logging icon and enable security intelligence logging using the following criteria:

- By Domain Name—Click the logging icon next to the **DNS Policy** drop-down list.
- By IP address—Click the logging icon next to **Networks**.
- By URL—Click the logging icon next to **URLs**.

c) Click **Save**.

Step 6 Enable syslog logging for each rule in the access control policy:

a) In the same access control policy, click the **Access Control** tab.

b) Click a rule to edit.

c) Click the **Logging** tab in the rule.

d) Check the **Log at beginning of connection** and **Log at end of connection** check boxes.

e) If you want to log file events, check the **Log Files** check box.

f) Check the **Syslog Server** check box.

g) Verify that the rule is **Using default syslog configuration in Access Control Logging**.

h) Click **Confirm**.

i) Click **Apply** to save the rule.

j) Repeat steps 7.a through 7.h for each rule in the policy and click **Save** to save the policy.

What to do next

If you have made all the required changes, deploy your changes to the managed devices.

Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection

Configure the cloud-delivered Firewall Management Center to send events directly to SAL (SaaS). Follow this procedure to enable the Cisco cloud event global setting in the cloud-delivered Firewall Management Center. When needed, you can exclude individual FTD devices from sending event logs to SAL (SaaS). For more information, see Enable or Disable Threat Defense Devices to Send Event logs to SAL (SaaS) Using a Direct Connection.

Before you begin

- Onboard devices to the cloud-delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **Integrations & Migration** > **Cloud Services**.

Step 3 Click **Cloud-Delivered FMC**, and in the **System** pane that is located at the right-side, click **Cisco Cloud Events**.

Step 4 In the **Configure Cisco Cloud Events** widget, do the following:

a. Click the **Send Events to the Cisco Cloud** toggle button to enable the overall configuration.

b. Check the **Send Intrusion Events to the cloud** check box to send the intrusion events to the cloud.

c. Check the **Send File and Malware Events to the cloud** check box to send the file and malware events to the cloud.

d. Choose an option to send the connection events to the cloud:

- Click the **None** radio button to not send connection events to the cloud.
- Click the **Security Events** radio button to send only security intelligence events to the cloud.
- Click the **All** radio button to send all the connection events to the cloud.

e. Click **Save**.

Enable or Disable Threat Defense Devices to Send Event logs to SAL (SaaS) Using a Direct Connection

Enable or disable the FTD devices managed by the cloud-delivered Firewall Management Center to send events directly to SAL (SaaS). This device-level control allows you to optionally exclude specific FTD devices from sending event logs to the Cisco cloud to reduce traffic or to maintain a combination of SAL and on-premises event log storage.

Note

- To enable or disable sending events to the Cisco cloud from the FTD devices, enable the Cisco cloud event global setting in the cloud-delivered Firewall Management Center. For more information on enabling the Cisco cloud event global setting, see Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection, on page 624.

  Sending events to the Cisco cloud is enabled by default for all FTD devices when the Cisco cloud event global setting is enabled in the cloud-delivered Firewall Management Center.

- The option to enable or disable FTD devices to send event logs to the cloud is supported on FTD Version 7.4.1 or later.

Before you begin

- Onboard devices to the cloud-delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 From the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to view the device.

Step 4 Click the **FTD** tab to view FTD devices.

Step 5 Choose the FTD devices whose configurations you want to edit, from the inventory list.

Step 6 In the **Device Management** pane, click **Cloud Events**.

Step 7 Click the **Send Events to the Cisco Cloud** toggle button to enable or disable the configuration.

Step 8 Click **Save**.

Secure Event Connectors

The Secure Event Connector (SEC) is a component of the Security Analytics and Logging SaaS solution. It receives events from ASA , and FDM-managed devices and forwards them to the Cisco cloud. Security Cloud Control displays the events on the Event Logging page so that administrators can analyze them there or by using Cisco Secure Cloud analytics.

The SEC is installed on a Secure Device Connector deployed in your network, on its own Security Cloud Control Connector virtual machine deployed in your network, or on an AWS Virtual Private Cloud (VPC).

Secure Event Connector ID

You may need the ID of the SEC when working with Cisco Technical Assistance Center (TAC) or other Security Cloud Control Support. That ID is found on the Secure Connectors page in Security Cloud Control. To find the SEC ID:

1. From the Security Cloud Control menu on the left, choose **Tools & Services** > **Secure Connectors**.
2. Click the SEC you wish to identify.
3. The SEC ID is the ID listed above the Tenant ID in the Details pane.

Related Information:

- Secure Logging Analytics for FDM-Managed Devices
- Install a Secure Event Connector on an SDC Virtual Machine, on page 627
- Install an SEC Using Your VM Image
- Install an SEC Using Your VM Image
- Install a Secure Event Connector on an AWS VPC Using a Terraform Module, on page 645
- Remove the Secure Event Connector
- Deprovisioning Cisco Security Analytics and Logging (SaaS)

Installing Secure Event Connectors

Secure Event Connectors (SECs) can be installed on a tenant with or without an SDC.

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own Security Cloud Control Connector virtual machine that you maintain in your network.

See these topics that describe the various installation cases:

- Install an SEC Using Your VM Image, on page 637
- Installing an SEC Using a Security Cloud Control Image, on page 630
- Install a Secure Event Connector on an AWS VPC Using a Terraform Module, on page 645

Install a Secure Event Connector on an SDC Virtual Machine

The Secure Event Connector (SEC) receives events from ASA and FDM-managed devices and forwards them to the Cisco cloud. Security Cloud Control displays the events on the Event Logging page so that administrators can analyze them there or by using Cisco Secure Cloud Analytics.

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own Security Cloud Control Connector virtual machine that you maintain in your network.

This article describes installing an SEC on the same virtual machine as an SDC. If you want to install more SECs see Installing an SEC Using a Security Cloud Control Image, on page 630 or Install an SEC Using Your VM Image, on page 637.

Before you begin

- Purchase the Cisco Security and Analytics Logging, **Logging and Troubleshooting** license. Or, If you want to try Cisco Security and Analytics Logging out first, log in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** and click **Request Trial**. You may also purchase the Logging **Analytics and Detection** and **Total Network Analytics and Monitoring** licenses to apply Secure Cloud Analytics to the events.
- Make sure your SDC has been installed. If you need to install an SDC, follow one of these procedures:
  - Deploy a Secure Device Connector Using Security Cloud Control's VM Image, on page 17
  - Deploy a Secure Device Connector On Your VM

Note If you installed the on-premises SDC on your own VM, there is Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created required to allow events to reach it.

- Make sure the SDC is communicating with Security Cloud Control:
  1. In the left pane, click **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.
  2. Make sure that the SDC's last heartbeat was less than 10 minutes prior to the installation of the SEC and that the SDC's status is active.
- System Requirements - Assign additional CPUs and memory to the virtual machine running the SDC:
  - CPU: Assign an **additional** 4 CPUs to accommodate the SEC to make a total of 6 CPU.
  - Memory: Assign an **additional** 8 GB of memory for the SEC to make a total of 10 GB of memory.

    After you have updated the CPU and memory on the VM to accommodate the SEC, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.

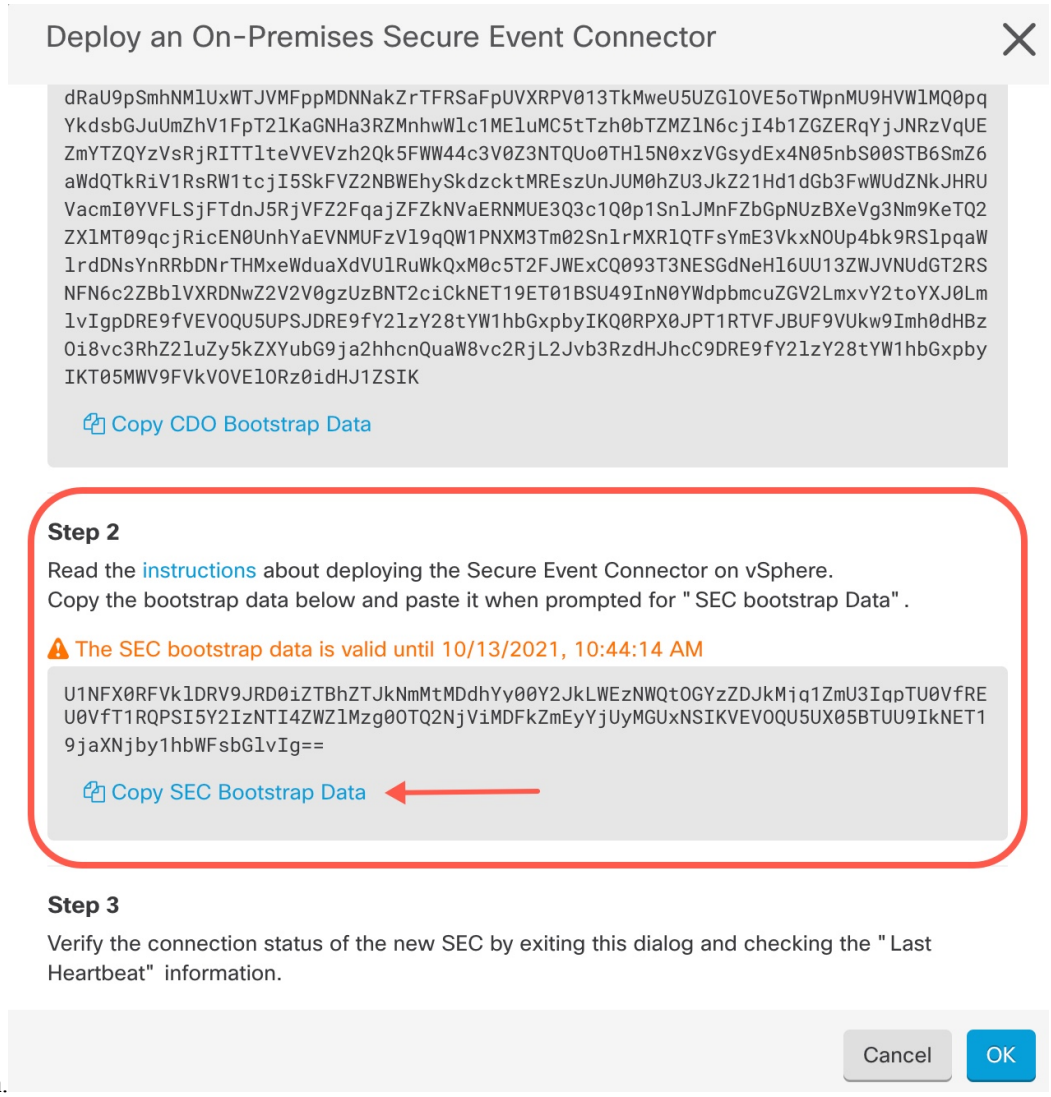
Procedure

Step 1 Log in to Security Cloud Control.

Step 2 From the left pane, click **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Click the  icon and then click **Secure Event Connector**.

Step 4 Skip Step 1 of the wizard and go to Step 2. In step 2 of the wizard, click the link to **Copy SEC Bootstrap Data**.



Step 5 Open a terminal window and log into the SDC as the "cdo" user.

Step 6 Once logged in, switch to the "sdc" user. When prompted for a password, enter the password for the "cdo" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

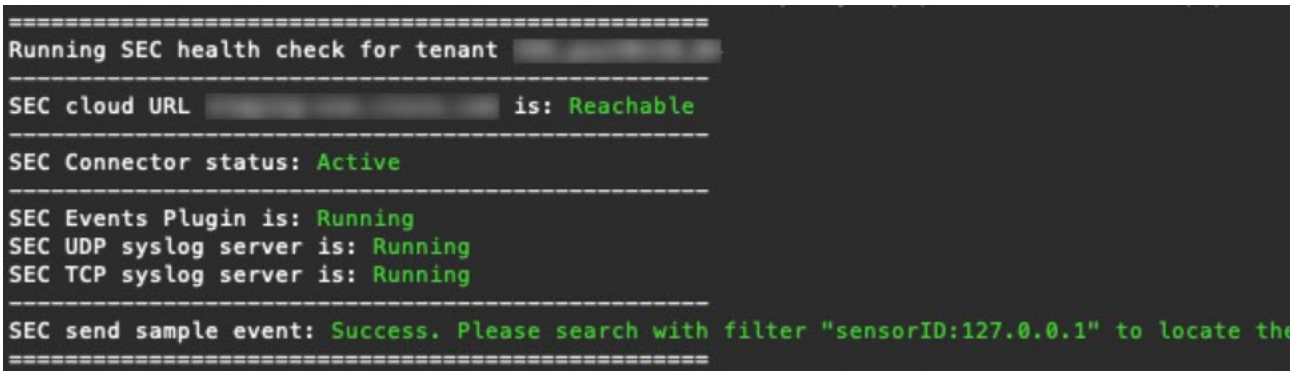
Step 7 At the prompt, run the **sec.sh setup** script:

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 8 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

```
Please copy the bootstrap data from Setup Secure Event Connector page of Security Cloud
Control: KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the sec.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "sec-health-check."



If you receive a message that the registration failed or that the SEC onboarding failed, go to Troubleshooting SEC Onboarding Failures.

Step 9 Determine if the VM on which the SDC and SEC are running needs additional configuration:

- If you installed your SDC on your own virtual machine, continue with Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created, on page 642.
- If you installed your SDC using a Security Cloud Control image, continue to "What to do Next."

What to do next

Return to Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices, on page 614.

Related Information:

- Troubleshoot a Secure Device Connector, on page 725
- Secure Event Connector Troubleshooting
- Troubleshooting SEC Onboarding Failures
- Troubleshooting Secure Event Connector Registration Failure, on page 736

Installing an SEC Using a Security Cloud Control Image

The Secure Event Connector (SEC) forwards events from ASA and FTD to the Cisco cloud so that you can view them in the Event Logging page and investigate them with Secure Cloud Analytics, depending on your licensing.

You can install more than one Secure Event Connector (SEC) on your tenant and direct events from your ASAs and FDM-managed devices to any of the SECs you install. Having multiple SECs allows you to have SECs installed in different locations and distribute the work of sending events to the Cisco cloud.

Installing an SEC is a two part process:

1. Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image, on page 631 You need one Security Cloud Control Connector for every SEC you install. The Security Cloud Control Connector is different than a Secure Device Connector (SDC).
2. Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine, on page 643.

Note If you want to create a Security Cloud Control Connector by creating your own VM, see Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created.

What to do next:

Continue with Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image, on page 631

Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image

Before you begin

- Purchase the Cisco Security and Analytics Logging, **Logging and Troubleshooting** license, you may also purchase the **Logging Analytics and Detection** and **Total Network Analytics and Monitoring** licenses to apply Secure Cloud Analytics to the events.

  If you would rather, you can request a trial version of Security Analytics and Logging by logging in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** and click **Request Trial**.

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the Security Cloud Control Connector and the Internet. If using a proxy server, disable inspection for traffic between the Security Cloud Control Connector and Security Cloud Control.
- **The** Security Cloud Control **Connector installed in this process must have full outbound access to the Internet on TCP port 443.**
- **Review** Connect Security Cloud Control to your Managed Devices **to ensure proper network access for the** Security Cloud Control **Connector.**
- Security Cloud Control supports installing its Security Cloud Control Connector VM OVF image using the vSphere web client or the ESXi web client.
- Security Cloud Control does not support installing the Security Cloud Control Connector VM OVF image using the VM vSphere desktop client.
- ESXi 5.1 hypervisor.
- System requirements for a VM intended to host only a Security Cloud Control Connector and an SEC:
  - VMware ESXi host needs 4 vCPU.
  - VMware ESXi host needs a minimum of 8 GB of memory.
  - VMware ESXi requires 64GB disk space to support the virtual machine depending on your provisioning choice.

- Gather this information before you begin the installation:
  - Static IP address you want to use for your Security Cloud Control Connector VM.
  - Passwords for the **root** and Security Cloud Control users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the SDC address is on.
  - The FQDN or IP address of your time server.
- The Security Cloud Control Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

Procedure

Step 1 Log on to the Security Cloud Control tenant you are creating the Security Cloud Control Connector for.

Step 2 In the left pane, click **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Click the + icon and then click **Secure Event Connector**.

Step 4 In Step 1, click **Download the** Security Cloud Control **Connector VM image**. This is a special image that you install the SEC on. Always download the Security Cloud Control Connector VM to ensure that you are using the latest image.

Step 5 Extract all the files from the .zip file. They will look similar to these:

- Security Cloud Control-SDC-VM-ddd50fa.ovf
- Security Cloud Control-SDC-VM-ddd50fa.mf
- Security Cloud Control-SDC-VM-ddd50fa-disk1.vmdk

Step 6 Log on to your VMware server as an administrator using the vSphere Web Client.

Note Do not use the VM vSphere desktop client.

Step 7 Deploy the on-premises Security Cloud Control Connector virtual machine from the OVF template by following the prompts. (You will need the .ovf, .mf, and .vdk files to deploy the template.)

Step 8 When the setup is complete, power on the VM.

Step 9 Open the console for your new Security Cloud Control Connector VM.

Step 10 Login as the Security Cloud Control user. The default password is `adm123`.

Step 11 At the prompt type `sudo sdc-onboard setup`

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

Step 12 When prompted, enter the default password for the Security Cloud Control user: `adm123`.

Step 13 Follow the prompts to create a new password for the **root** user.

Step 14 Follow the prompts to create a new password for the Security Cloud Control user.

Step 15 Follow the prompts to enter your Security Cloud Control domain information.

Step 16 Enter the static IP address you want to use for the Security Cloud Control Connector VM.

Step 17 Enter the gateway IP address for the network on which the Security Cloud Control Connector VM is installed.

Step 18 Enter the NTP server address or FQDN for the Security Cloud Control Connector.

Step 19 When prompted, enter the information for the Docker bridge or leave it blank if it is not applicable and press <Enter>.

Step 20 Confirm your entries.

Step 21 When prompted "Would you like to setup the SDC now?" enter **n**.

Step 22 Create an SSH connection to the Security Cloud Control Connector by logging in as the Security Cloud Control user.

Step 23 At the prompt type **`sudo sdc-onboard bootstrap`**

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

Step 24 When prompted, enter the Security Cloud Control user's password.

Step 25 When prompted, return to Security Cloud Control and copy the Security Cloud Control bootstrap data, then paste it into your SSH session. To copy the Security Cloud Control bootstrap data:

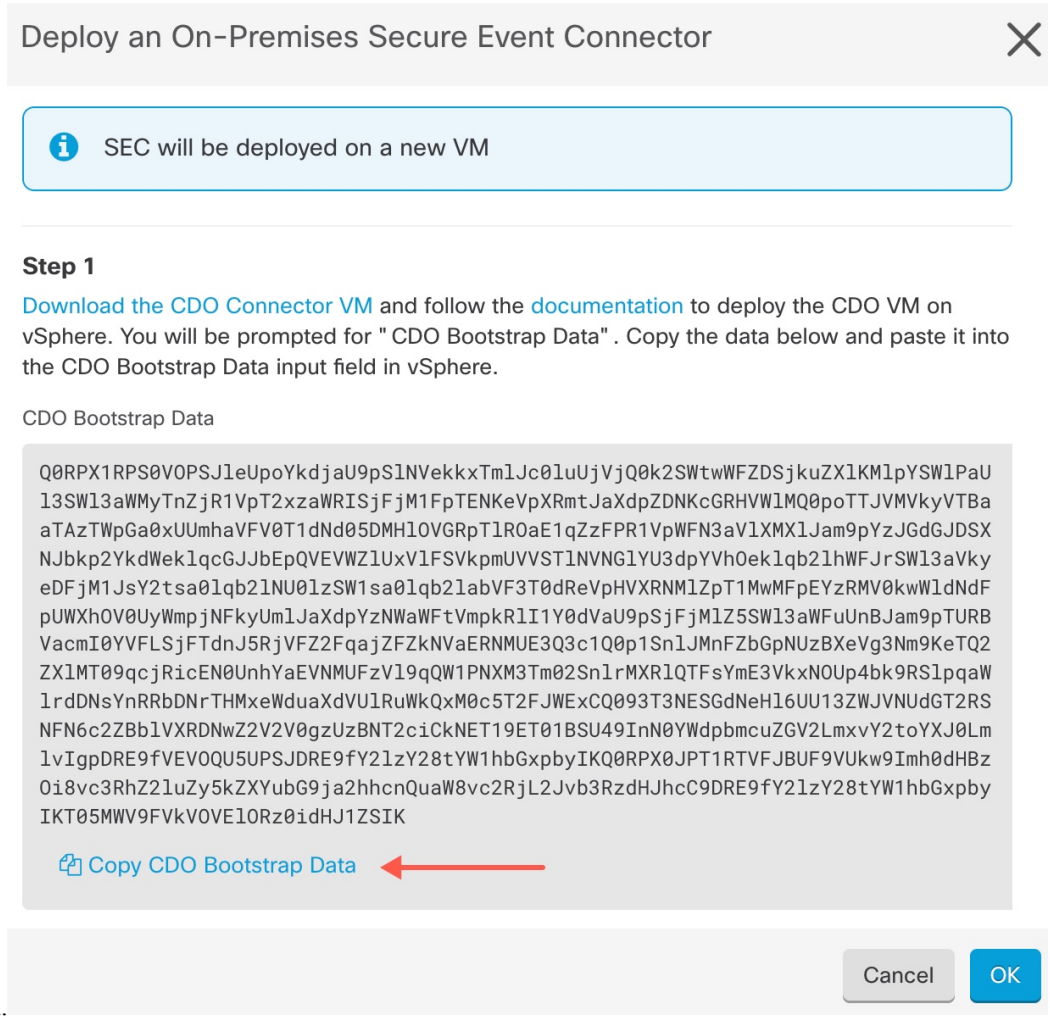
a. Log into Security Cloud Control.

b. In the left pane, click **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

c. Select the Secure Event Connector which you started to onboard. The status should show, "Onboarding."

d. In the **Actions** pane, click **Deploy an On-Premises Secure Event Connector**.

e. Copy the Security Cloud Control Bootstrap Data in step 1 of the dialog box.



Step 26 When prompted, **Would you like to update these settings?** enter **n**.

Step 27 Return to the Deploy an On-Premises Secure Event Connector dialog in Security Cloud Control and click **OK**. On the Secure Connectors page, you see your Secure Event Connector is in the yellow Onboarding state.

What to do next

Continue to Install the Secure Event Connector on the Security Cloud Control Connector VM, on page 634.

Install the Secure Event Connector on the Security Cloud Control Connector VM

Before you begin

You should have installed Security Cloud Control Connector VM as described inInstall a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image, on page 631 .

Procedure

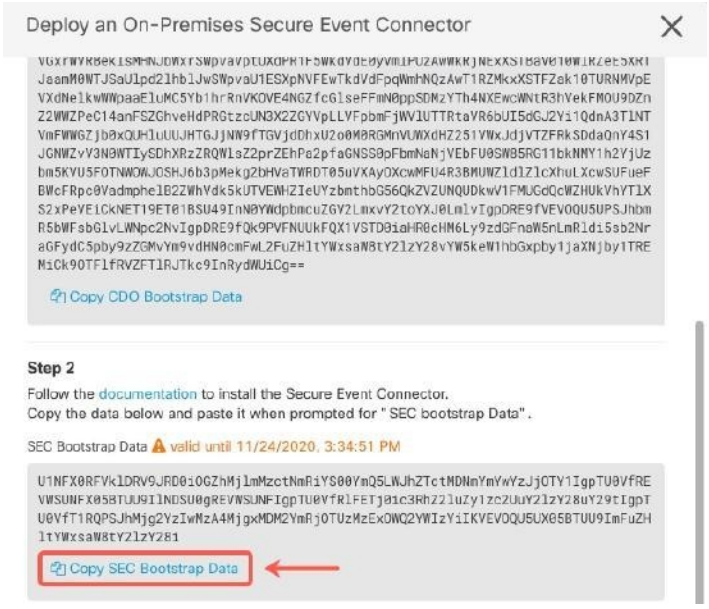
Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, choose **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Select the Security Cloud Control Connector that you onboarded above. In the Secure Connectors table, it will be called a Secure Event Connector and it should still be in the "Onboading" status.

Step 4 Click **Deploy an On-Premises Secure Event Connector** in the Actions pane on the right.

Step 5 In **step 2** of the wizard, click the link to **Copy SEC bootstrap data**.



Step 6 Create an SSH connection to the Security Cloud Control Connector and log in as the Security Cloud Control user.

Step 7 Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "Security Cloud Control" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

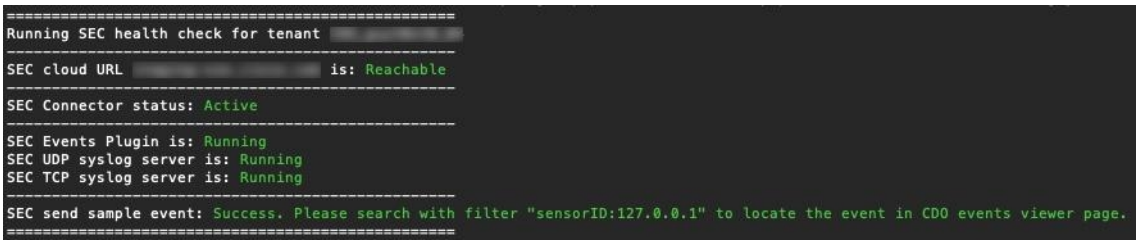
Step 8 At the prompt, run the sec.sh setup script:

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 9 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the sec.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "sec-health-check."



If you receive a message that the registration failed or that the SEC onboarding failed, go to Troubleshooting SEC Onboarding Failures, on page 733.

If you receive the success message return to Security Cloud Control and click **Done on the Deploy an ON-Premise Secure Event Connector** dialog box.

What to do next

Return to Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices, on page 614.

Related Information:

- Troubleshoot a Secure Device Connector, on page 725
- Secure Event Connector Troubleshooting, on page 733
- Troubleshooting SEC Onboarding Failures, on page 733

Deploy Secure Event Connector on Ubuntu Virtual Machine

Before you begin

You should have installed Secure Device Connector on your Ubuntu VM as described in Deploy Secure Device Connector and Secure Event Connector on Ubuntu Virtual Machine, on page 25.

Procedure

Step 1 Log on to Security Cloud Control.

Step 2 From the left pane, **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Click the  icon and then click **Secure Event Connector**.

Step 4 Copy the SEC bootstrap data in step 2 on the window to a notepad.

Step 5 Execute the following commands:

```
[sdc@vm]:~$sudo su sdc
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

When prompted, enter the SEC bootstrap data that you have copied..

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

It may take a few minutes for the Secure Event Connector to become "Active" in Security Cloud Control.

Install an SEC Using Your VM Image

The Secure Event Connector (SEC) forwards events from ASA and FTD to the Cisco cloud so that you can view them in the Event Logging page and investigate them with Secure Cloud Analytics, depending on your licensing.

You can install more than one Secure Event Connector (SEC) on your tenant and direct events from your ASAs and FDM-managed devices to any of the SECs you install. Having multiple SECs allows you to have SECs installed in different regions and distribute the work of sending events to the Cisco cloud.

Installing multiple SECs using your own VM image is a three part process. You must perform each of these steps:

1. Install a Security Cloud Control Connector to Support an SEC Using Your VM Image, on page 637
2. Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created, on page 642
3. Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine

Note Using a Security Cloud Control VM image for the Security Cloud Control Connector is the easiest, most accurate, and preferred method of installing a Security Cloud Control connector. If you want to use that method, see Installing an SEC Using a Security Cloud Control Image, on page 630.

What to do next:

Continue to Install a Security Cloud Control Connector to Support an SEC Using Your VM Image, on page 637

Install a Security Cloud Control Connector to Support an SEC Using Your VM Image

The Security Cloud Control Connector VM is a virtual machine on which you install an SEC. The purpose of the Security Cloud Control Connector is solely to support an SEC for Cisco Security Analytics and Logging (SaaS) customers.

This is the first of three steps you need to complete in order install and configure your Secure Event Connector (SEC). After this procedure, you need to complete the following procedures:

- Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created, on page 642
- Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine

Before you begin

- Purchase the Cisco Security and Analytics Logging, **Logging and Troubleshooting**license, you may also purchase the **Logging Analytics and Detection** and **Total Network Analytics and Monitoring** licenses to apply Secure Cloud Analytics to the events.

  If you would rather, you can request a trial version of Security Analytics and Logging by logging in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** and click **Request Trial**.

- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the Security Cloud Control Connector and the Internet.
- **The Security Cloud Control Connector must have full outbound access to the Internet on TCP port 443.**
- **Review** Connect Security Cloud Control to your Managed Devices**to ensure proper network access for the Security Cloud Control Connector.**
- VMware ESXi host installed with vCenter web client or ESXi web client.

Note We do not support installation using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Cent OS 7 guest operating system.
- System requirements for a VM to host only a Security Cloud Control Connector and an SEC:
  - CPU: Assign 4 CPUs to accommodate the SEC.
  - Memory: Assign 8 GB of memory for the SEC.
  - Disk Space: 64 GB
- Users performing this procedure should be comfortable working in a Linux environment and using the **vi** visual editor for editing files.
- If you are installing your Security Cloud Control Connector on a CentOS virtual machine, we recommend you install Yum security patches on a regular basis. Depending on your Yum configuration, to acquire Yum updates, you may need to open outbound access on port 80 as well as 443. You will also need to configure yum-cron or crontab to schedule the updates. Work with your security-operations team to determine if any security policies need to change to allow you to get the Yum updates.
- Gather this information before you begin the installation:
  - Static IP address you want to use for your Security Cloud Control Connector.
  - Passwords for the **root** and **Security Cloud Control** users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the Security Cloud Control Connector address is on.
  - The FQDN or IP address of your time server.

- The Security Cloud Control Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.
- **Before you get started**: Do not copy and paste the commands in this procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

Procedure

Step 1 Log on to Security Cloud Control.

Step 2 From the left pane, **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Click the  icon and then click **Secure Event Connector**.

Step 4 Using the link provided, copy the SEC Bootstrap Data in step 2 of the "Deploy an On-Premises Secure Event Connector" window.

Step 5 Install a CentOS 7 virtual machine (http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso) with at least the memory, CPU, and disk space mentioned in this procedure's perquisites.

Step 6 Once installed, configure basic networking such as specifying the IP address for the Security Cloud Control Connector, the subnet mask, and gateway.

Step 7 Configure a DNS (Domain Name Server) server.

Step 8 Configure a NTP (Network Time Protocol) server.

Step 9 Install an SSH server on CentOS for easy interaction with Security Cloud Control Connector's CLI.

Step 10 Run a Yum update and then install the packages: **open-vm-tools**, **nettools**, and **bind-utils**

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

Step 11 Install the **AWS CLI package** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)

Note Do not use the `--user` flag.

Step 12 Install the **Docker CE packages** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)

Note Use the "Install using the repository" method.

Step 13 Start the Docker service and enable it to start on boot:

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

Step 14 Create two users: **Security Cloud Control** and **sdc.** The Security Cloud Control user will be the one you log-into to run administrative functions (so you don't need to use the root user directly), and the sdc user will be the user to run the Security Cloud Control Connector docker container.

```
[root@sdc-vm ~]# useraddSecurity Cloud Control
 [root@sdc-vm ~]# useradd sdc -d /usr/local/Security Cloud Control
```

Step 15 Configure the sdc user to use crontab:

```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```

Step 16 Set a password for the Security Cloud Control user.

```
[root@sdc-vm ~]# passwd Security Cloud Control
Changing password for user Security Cloud Control.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

Step 17 Add the Security Cloud Control user to the "wheel" group to give it administrative (sudo) privileges.

```
[root@sdc-vm ~]# usermod -aG wheelSecurity Cloud Control
 [root@sdc-vm ~]#
```

Step 18 When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

Step 19 If the `/etc/docker/daemon.json` file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

Note Make sure that the group name entered in the "group" key matches the Step 18.

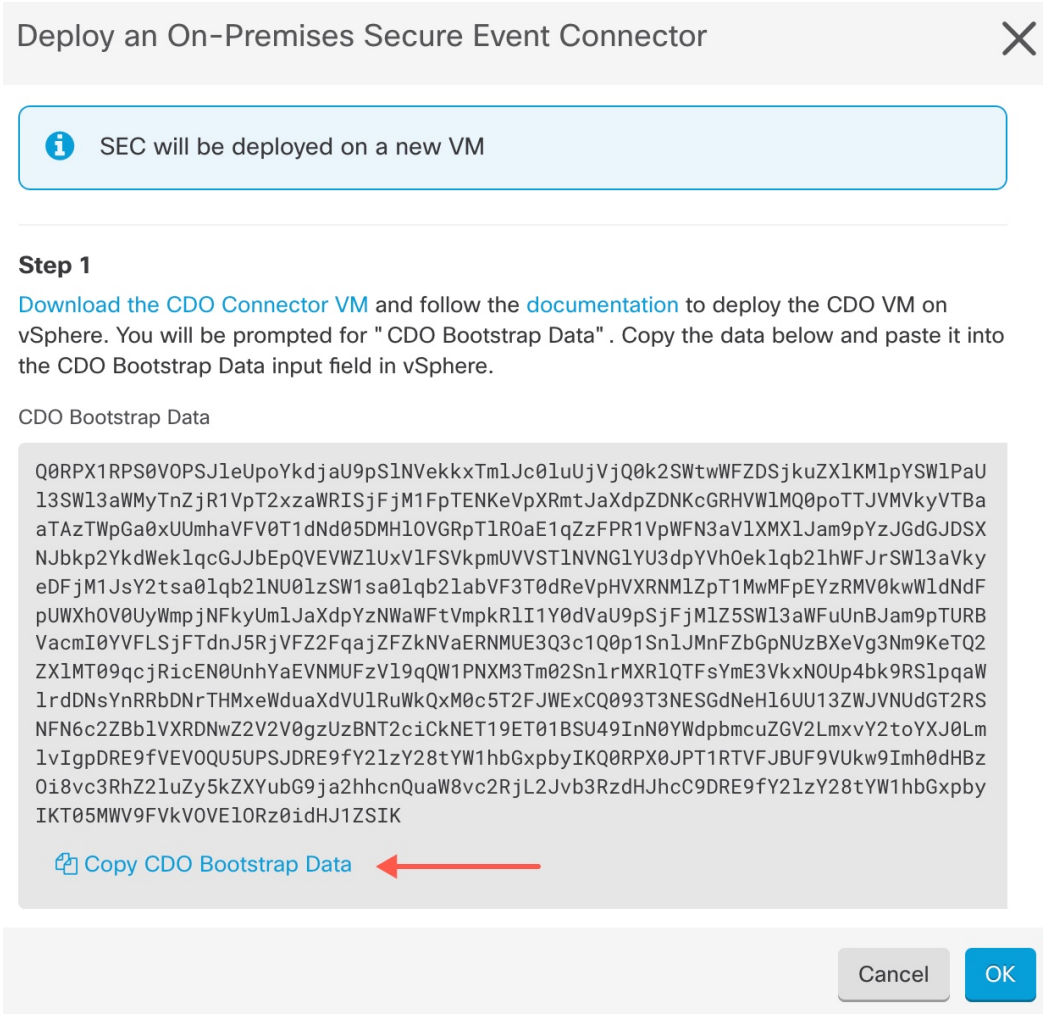
```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

Step 20 If you are currently using a vSphere console session, switch over to SSH and log in as the **Security Cloud Control** user. Once logged in, change to the **sdc** user. When prompted for a password, enter the password for the **Security Cloud Control** user.

```
[Security Cloud Control@sdc-vm ~]$ sudo su sdc
[sudo] password for Security Cloud Control: <type password for Security Cloud Control user
 >
[sdc@sdc-vm ~]$
```

Step 21 Change directories to **/usr/local/**Security Cloud Control**.**

Step 22 Create a new file called **bootstrapdata** and paste the bootstrap data from Step 1 of the deployment wizrd into this file. **Save** the file. You can use **vi** or **nano** to create the file.



Step 23 The bootstrap data comes encoded in base64. Decode it and export it to a file called **extractedbootstrapdata**

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/Security Cloud Control/bootstrapdata >
/usr/local/Security Cloud Control/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

Run the cat command to view the decoded data. The command and decoded data should look similar to this:

```
[sdc@sdc-vm ~]$ cat /usr/local/Security Cloud Control/extractedbootstrapdata
Security Cloud Control_TOKEN="<token string>"
Security Cloud Control_DOMAIN="www.defenseorchestrator.com"
Security Cloud Control_TENANT="<tenant-name>"
<Security Cloud Control_URL>/sdc/bootstrap/Security Cloud
Control_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

Step 24 Run the following command to export the sections of the decoded bootstrap data to environment variables.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > secenv && source secenv
[sdc@sdc-vm ~]$
```

Step 25 Download the bootstrap bundle from Security Cloud Control.

```
 [sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $Security Cloud Control_TOKEN" "$Security
Cloud Control_BOOTSTRAP_URL" -o $Security Cloud Control_TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/Security Cloud Control/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/Security Cloud Control/Security Cloud
Control_<tenant_name>
```

Step 26 Extract the Security Cloud Control Connector tarball, and run the bootstrap_sec_only.sh file to install the Security Cloud Control Connector package.

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/Security Cloud Control/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/Security Cloud Control/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/Security Cloud Control/toolkit/es_toolkit.sh upgradeEventing 2>&1
>> /usr/local/Security Cloud Control/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/Security Cloud Control/toolkit/es_toolkit.sh es_maintenance
 2>&1 >> /usr/local/Security Cloud Control/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

What to do next

Continue to Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created, on page 642 .

Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created

If you installed your Security Cloud Control Connector on your own CentOS 7 virtual machine, perform one of the following additional configuration procedures to allow events to reach the SEC:

- Disable the firewalld service on the CentOS 7 VM: This matches the configuration of the Cisco-provided SDC VM.
- Allow the firewalld service to run and add firewall rules to allow event traffic to reach the SEC, on page 643: This is a more granular approach to allowing inbound event traffic.

Before you begin:

This is the second of three steps you need to complete in order to install and configure your SEC. If you have not already, complete Install a Security Cloud Control Connector to Support an SEC Using Your VM Image, on page 637 before making these configuration changes.

After you complete one of the additional configuration changes described here, complete Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine

Disable the firewalld service on the CentOS 7 VM

1. Log into the CLI of the SDC VM as the "Security Cloud Control" user.
2. Stop the firewalld service, and then ensure that it will remain disabled upon subsequent reboots of the VM. If you are prompted, enter the password for the **Security Cloud Control** user:

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl stop firewalld
Security Cloud Control@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Restart the Docker service to re-insert Docker-specific entries into the local firewall:

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart docker
```

4. Continue to Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine.

Allow the firewalld service to run and add firewall rules to allow event traffic to reach the SEC

1. Log into the CLI of the SDC VM as the "Security Cloud Control" user.
2. Add local firewall rules to allow incoming traffic to the SEC from the TCP, UDP, or NSEL ports you configured. See Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS) for the ports used by your SEC. If prompted, enter the password for the **Security Cloud Control** user. Here is an example of the commands. You may need to specify different port values.

```
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10125/tcp
Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10025/udp
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10425/udp
```

3. Restart the firewalld service to make the new local firewall rules both active and persistent:

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. Continue to Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine.

Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine

Before you begin

This is the third of three steps you need to complete in order to install and configure your Secure Event Connector (SEC). If you have not already, complete the following tasks before continuing with this procedure:

- Install a Security Cloud Control Connector to Support an SEC Using Your VM Image, on page 637.
- Additional Configuration for SDCs and Security Cloud Control Connectors Installed on a VM You Created, on page 642.

Procedure

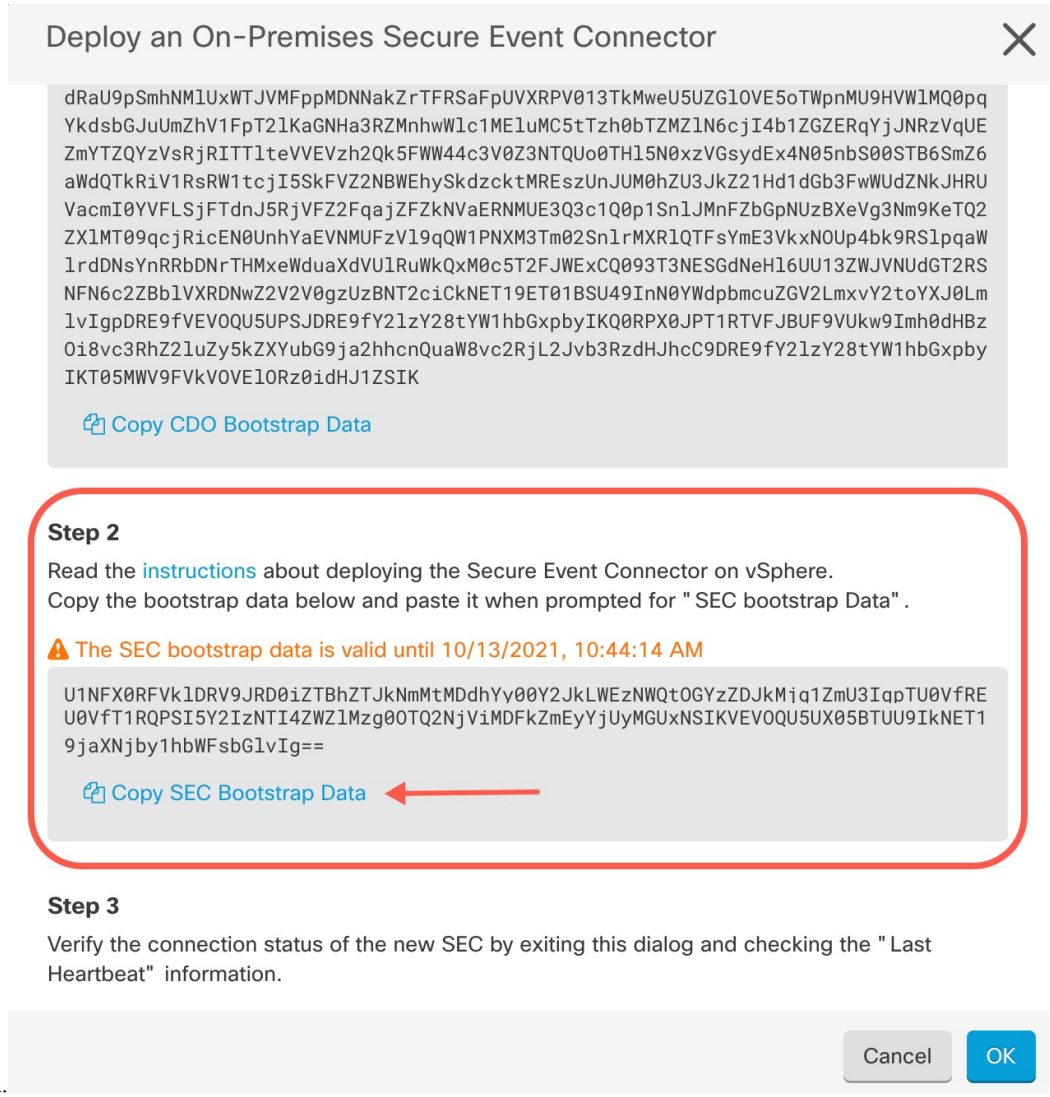
Step 1 Log in to Security Cloud Control.

Step 2 From the left pane, **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Select the Security Cloud Control Connector that you installed using the procedure in the prerequisites above. In the Secure Connectors table, it will be displayed as Secure Event Connector.

Step 4 Click **Deploy an On-Premises Secure Event Connector** in the **Actions** pane on the right.

Step 5 In **step 2** of the wizard, click the link to **Copy SEC Bootstrap Data**.



Step 6 Connect to the Secure Connector using SSH and log in as the Security Cloud Control user.

Step 7 Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "Security Cloud Control" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

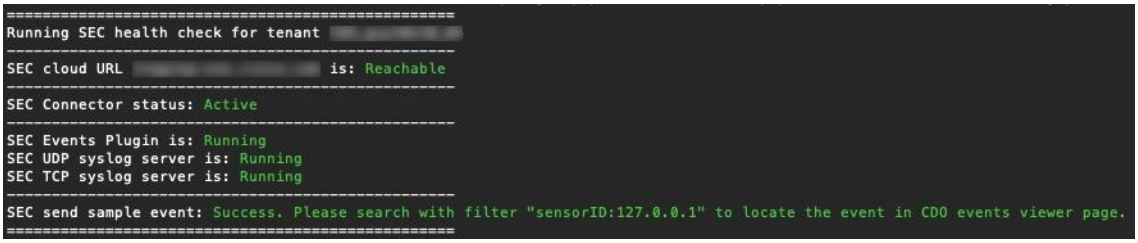
Step 8 At the prompt, run the sec.sh setup script:

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 9 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the sec.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "sec-health-check."



If you receive a message that the registration failed or that the SEC onboarding failed, go to Secure Event Connector Troubleshooting.

If you receive the success message, click **Done** in the **Deploy an ON-Premise Secure Event Connector** dialog box.You have finished installing an SEC on a your VM image.

What to do next

Return to this procedure to continue your implementation of SAL SaaS: Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices, on page 614.

Related Information:

- Troubleshoot a Secure Device Connector, on page 725
- Secure Event Connector Troubleshooting
- Troubleshooting SEC Onboarding Failures
- Troubleshooting Secure Event Connector Registration Failure

Install a Secure Event Connector on an AWS VPC Using a Terraform Module

Before you begin

- To perform this task, you must enable SAL on your Security Cloud Control tenant. This section presumes that you have a SAL license. If you do not have one, purchase the Cisco Security and Analytics Logging, Logging and Troubleshooting license.
- Ensure you have a new SEC installed. To create a new SEC, see Install a Secure Event Connector on an SDC Virtual Machine, on page 627.
- When installing the SEC, make sure you take a note of the Security Cloud Control bootstrap data and SEC bootstrap data.

Procedure

Step 1 Go to Secure Event Connector Terraform Module on the Terraform Registry and follow the instructions to add the SEC Terraform module to your Terraform code.

Step 2 Apply the Terraform code.

Step 3 Ensure that you print the `instance_id` and `sec_fqdn` outputs, because you will need them later in the procedure.

Note To troubleshoot your SEC, you must connect to your SEC instance using the AWS Systems Manager Session Manager (SSM). See the AWS Systems Manager Session Manager documentation to know more about connecting to an instance using SSM.

Ports to connect to the SDC instance using SSH are not exposed for secuirty reasons.

Step 4 To enable sending of logs from your ASA to the SEC, obtain the certificate chain of the SEC you created and remove the leaf certificate by running the following command with the output from Step 3:

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 <
 /dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++};
out="/tmp/cert_chain.pem"; if(a > 1) print >>out}'
```

Step 5 Copy the contents of `/tmp/cert_chain.pem` to your clipboard.

Step 6 Take a note of the IP address of the SEC using the following command:

```
nslookup <FQDN>
```

Step 7 Log in to Security Cloud Control and start adding a new trustpoint object. See Adding a Trusted CA Certificate Object for more information. Ensure you uncheck the **Enable CA flag in basic constraints extension** checkbox in **Other Options** before clicking **Add**.

Step 8 Click **Add**, copy the CLI commands generated by Security Cloud Control in the **Install Certificate** page, and click **Cancel**.

Step 9 Below `enrollment terminal`, add `no ca-check` in a text clipboard.

Step 10 SSH into your ASA device or use the ASA CLI option in Security Cloud Control and execute the following commands:

```
DataCenterFW-1> en
Password: *****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

What to do next

You can check if your SEC is receiving packets using AWS SSM:

You should now see logs similar to this:

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

Deprovisioning Cisco Security Analytics and Logging (SaaS)

If you allow your Cisco Security Analytics and Logging (SaaS) paid license to lapse, you have a grace period of 90 days. If you renew your paid license during this grace period, there is no interruption in your service.

Otherwise, if you allow the 90-day grace period to elapse, the system purges all of your customer data. You can no longer view ASA or FTD events from the Event Logging page, nor have dynamic entity modeling behavioral analytics applied to your ASA or FTD events and network flow data.

Remove the Secure Event Connector

Warning: This procedure deletes the Secure Event Connector from the Secure Device Connector. Doing so will prevent you from using Secure Logging Analytics (SaaS). It is not reversible. If you have any questions or concerns, Contact Security Cloud Control Support before taking this action.

Removing the Secure Event Connector from your Secure Device Connector is a two-step process:

1. Remove an SEC from Security Cloud Control.
2. Remove SEC files from the SDC.

What to do next: Continue to Remove an SEC from Security Cloud Control

Remove an SEC from Security Cloud Control

Before you begin

See Remove the Secure Event Connector, on page 647.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 From the left pane, choose **Administration** > **Integrations & Migration** > **Cloud Services** and then click the **Secure Connectors** tab.

Step 3 Select the row with the device type, **Secure Event Connector**.

Warning Be careful NOT to select your Secure Device Connector.

Step 4 In the **Actions** pane, click **Remove**.

Step 5 Click **OK** to confirm.

What to do next

Continue to Remove SEC files from the SDC, on page 648.

Remove SEC files from the SDC

This is the second part of a two part procedure to remove the Secure Event Connector from your SDC. See Remove the Secure Event Connector, on page 647 before you begin.

Procedure

Step 1 Open your virtual machine hypervisor and start a console session for your SDC.

Step 2 Switch to the SDC user.

```
[cdo@tenant toolkit]$sudo su sdc
```

Step 3 At the prompt type one of these commands:

- If you are managing only your own tenant:

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
  ```

- If you manage more than one tenant, add Security Cloud Control_ to the beginning of the tenant name. For example:

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
  ```

Step 4 Confirm your intention to remove the SEC files.

Provision a Cisco Secure Cloud Analytics Portal

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

If you purchase a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, after you deploy and configure the Secure Event Connector (SEC), you must associate a Secure Cloud Analytics portal with your Security Cloud Control portal to view Secure Cloud Analytics alerts. When you purchase the license, if you have an existing Secure Cloud Analytics portal, you can provide the Secure Cloud Analytics portal name and immediately link it to your Security Cloud Control portal.

Otherwise, you can request a new Secure Cloud Analytics portal from the Security Cloud Control UI. The first time you access Secure Cloud Analytics alerts, the system takes you to a page to request the Secure Cloud Analytics portal. The user that requests this portal is granted administrator permission in the portal.

Procedure

Step 1 In the left pane, click **Analytics** > **Secure Cloud Analytics** to open the Secure Cloud Analytics UI in a new window.

Step 2 Click **Start Free Trial** to provision a Secure Cloud Analytics portal and associate it with your Security Cloud Control portal.

Note After you request the portal, the provisioning may take up to several hours.

Ensure that your portal is provisioned before moving on to the next step.

1. In the left pane, click **Analytics** > **Secure Cloud Analytics** to open the Secure Cloud Analytis UI in a new window.
2. You have the following options:
   - If you requested a Secure Cloud Analytics portal, and the system states it is still provisioning the portal, wait and try to access the alerts later.
   - If the Secure Cloud Analytics portal is provisioned, enter your **Username** and **Password**, then click **Sign in**.

Note The administrator user can invite other users to create accounts within the Secure Cloud Analytis portal. See Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control, on page 651 for more information.

What to do next

- If you purchased a **Logging Analytics and Detection** license, your configuration is complete. If you want to view the status of your Security Cloud Control integration or sensor health from the Secure Cloud Analytics portal UI, see Review Sensor Health and Security Cloud Control Integration Status in Secure Cloud Analytics, on page 649 for more information. If you want to work with alerts in the Secure Cloud Analytics portal, see Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control, on page 651 and Working with Alerts Based on Firewall Events for more information.
- If you purchased a **Total Network Analytics and Monitoring** license, deploy one or more Secure Cloud Analytics sensors to your internal network to pass network flow data to the cloud. If you want to monitor cloud-based network flow data, configure your cloud-based deployment to pass flow data to Secure Cloud Analytics. See Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting, on page 650 for more information.

Review Sensor Health and Security Cloud Control Integration Status in Secure Cloud Analytics

Sensor Status

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

In the Secure Cloud Analytis web UI, you can view your Security Cloud Control integration status and your configured sensors from the Sensor List page. The Security Cloud Control integration is the read-only *connection-events* sensor. Stelathwatch Cloud provides an overall health of your sensors in the main menu:

- green cloud icon ( ) - connectivity established with all sensors, and Security Cloud Control if configured

- yellow cloud icon ( ) - connectivity established with some sensors, or Security Cloud Control if configured, and one or more sensors is not configured properly
- red cloud icon ( ) - connectivity lost with all configured sensors, and Security Cloud Control if configured

Per sensor or Security Cloud Control integration, a green icon signifies connectivity established, and a red icon signifies connectivity lost.

Procedure

Step 1 1. In the Secure Cloud Analytis portal UI, select **Settings ( ) > Sensors**.

Step 2 Select **Sensor List**.

Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting

Secure Cloud Analytics Sensor Overview and Deployment

Required License: **Total Network Analytics and Monitoring**

If you obtain a **Total Network Analytics and Monitoring** license, after you provision a Secure Cloud Analytics portal, you can:

- Deploy and configure a Secure Cloud Analytics sensor within your on-premises network to pass network flow data to the cloud for analysis.
- Configure your cloud-based deployment to pass network flow log data to Secure Cloud Analytics for analysis.

Firewalls at your network perimeter gather information about traffic between your internal network and external networks, while Secure Cloud Analytics sensors gather information about traffic within your internal network.

Note FDM-managedSecure Firewall Threat Defense devices may be configured to pass NetFlow data. When you deploy a sensor, do not configure it to pass NetFlow data from any of your FDM-managedSecure Firewall Threat Defense devices which you also configured to pass event information to Security Cloud Control.

See the Secure Cloud Analytics Sensor Installation Guide for sensor deployment instructions and recommendations.

See the Secure Cloud Analytics Public Cloud Monitoring Guides for cloud-based deployment configuration instructions and recommendations.

Note You can also review instructions in the Secure Cloud Analytics portal UI to configure sensors and your cloud-based deployment.

See the Secure Cloud Analytics Free Trial Guide for more information about Secure Cloud Analytics.

Next Steps

- Continue with Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control, on page 651.

Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

While you can review your firewall events on the Events logging page, you cannot review Cisco Secure Cloud Analytics alerts from the Security Cloud Control portal UI. You can cross-launch from Security Cloud Control to the Secure Cloud Analytics portal using the Security Analytics menu option, and view alerts generated from firewall event data (and from network flow data if you enabled **Total Network Analytics and Monitoring**). The Security Analytics menu option displays a badge with the number of Secure Cloud Analytics alerts in an open workflow status, if 1 or more are open.

If you use a Security Analytics and Logging license to generate Secure Cloud Analytics alerts, and you provisioned a new Secure Cloud Analytics portal, log into Security Cloud Control, then cross-launch to Secure Cloud Analytics using Cisco Security Cloud Sign On. You can also directly access your Secure Cloud Analytics portal through its URL.

See Cisco Security Cloud Sign On for more information.

Inviting Users to Join Your Secure Cloud Analytics Portal

The initial user to request the Secure Cloud Analytics portal provision has administrator privileges in the Secure Cloud Analytics portal. That user can invite other users by email to join the portal. If these users do not have Cisco Security Cloud Sign On credentials, they can create them using the link in the invite email. Users can then use Cisco Security Cloud Sign On credentials to log in during the cross-launch from Security Cloud Control to Secure Cloud Analytics.

To invite other users to your Secure Cloud Analytics portal by email:

Procedure

Step 1 Log into your Secure Cloud Analytics portal as an administrator.

Step 2 Select **Settings** > **Account Management** > **User Management**.

Step 3 Enter an **Email** address.

Step 4 Click **Invite**.

Cross-Launching from Security Cloud Control to Secure Cloud Analytics

To view security alerts from Security Cloud Control:

Procedure

Step 1 Log into the Security Cloud Control portal.

Step 2 In the left pane, choose **Analytics** > **Secure Cloud Analytics**.

Step 3 In the Secure Cloud Analytics interface, select **Monitor** > **Alerts**.

Cisco Secure Cloud Analytics and Dynamic Entity Modeling

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Secure Cloud Analytics is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Dynamic Entity Modeling

Dynamic entity modeling tracks the state of your network by performing a behavioral analysis on firewall events and network flow data. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they take on your network. Secure Cloud Analytics, integrated with a **Logging Analytics and Detection** license, can draw from firewall events and other traffic information in order to determine the types of traffic the entity usually transmits. If you purchase a **Total Network Analytics and Monitoring** license, Secure Cloud Analytics can also include NetFlow and other traffic information in modeling entity traffic. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity. From this information, Secure Cloud Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, or a remote access session established with another entity. If you

integrate with Security Cloud Control, these facts can be obtained from firewall events. If you also purchase a **Total Network Analytics and Monitoring**, license, the system can also obtain facts from NetFlow, and generate observations from both firewall events and NetFlow. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Alerts and Analysis

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system. Note that one alert may represent multiple observations. If a firewall logs multiple connection events related to the same connection and entities, this may result in only one alert.

For example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

Note that when you view and close alerts in Secure Cloud Analytics, you cannot allow or block traffic from the Secure Cloud Analytics UI. You must update your firewall access control rules to allow or block traffic, if you deployed your devices in active mode, or your firewall access control rules if your firewalls are deployed in passive mode.

Working with Alerts Based on Firewall Events

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alerts Workflow

An alert's workflow is based around its status. When the system generates an alert, the default status is Open, and no user is assigned. When you view the Alerts summary, all open alerts are displayed by default, as these are of immediate concern.

Note: If you have a **Total Network Analytics and Monitoring** license, your alerts can be based on observations generated from NetFlow, observations generated from firewall events, or observations from both data sources.

As you review the Alerts summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees. You can set an alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert, to display it as an open alert again. As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert. This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior.

As you research within the Secure Cloud Analytics web portal UI, in Security Cloud Control, and on your network, you can leave comments with the alert that describe your findings. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed, and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

The following presents general guidelines and suggestions for how to investigate a given alert. Because Secure Cloud Analytics provides additional context when it logs an alert, you can use this context to help guide your investigation.

These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

In general, you can take the following steps when you review an alert:

1. Triage open alerts, on page 654
2. Snooze alerts for later analysis, on page 655
3. Update the alert for further investigation, on page 655
4. Review the alert and start your investigation, on page 656
5. Examine the entity and users, on page 657
6. Remediate issues using Secure Cloud Analytics, on page 658
7. Update and close the alert, on page 658

Triage open alerts

Triage the open alerts, especially if more than one have yet to be investigated:

- See Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control for more information on cross-launching from Security Cloud Control to Secure Cloud Analytics, and viewing alerts.

Ask the following questions:

- Have you configured this alert type as high priority?
- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?

- If there is communication with external entities, have these entities established connections with other entities on your network in the past?

If this is a *high* priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

Snooze alerts for later analysis

Snooze alerts when they are of lesser priority, as compared to other alerts. For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert (indicating that an entity's current traffic matches a behavior profile that it did not previously match), you can snooze this alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

Snooze an alert:

Procedure

Step 1 Click **Close Alert**.

Step 2 In the Snooze this alert pane, select a snooze period from the drop-down.

Step 3 Click **Save**.

What to do next

When you are ready to review these alerts, you can unsnooze them. This sets the status to Open, and displays the alert alongside the other Open alerts.

Unsnooze a snoozed alert:

- From a snoozed alert, click **Unsnooze Alert**.

Update the alert for further investigation

Open the alert detail:

Procedure

Step 1 Select **Monitor** > **Alerts**.

Step 2 Click an alert type name.

What to do next

Based on your initial triage and prioritization, assign the alert and tag it:

1. Select a user from the **Assignee** drop-down to assign the alert, so a user can start investigating.

2. Select one or more **Tags** from the drop-down to add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.
3. Enter a **Comment on this alert**, then click **Comment** to leave comments as necessary to track your initial findings, and assist the person assigned to the alert. The alert tracks both system comments and user comments.

Review the alert and start your investigation

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert. Review the supporting observations to understand what these observations mean for the source entity.

Note that if the alert was generated based on firewall events, the system does not note that your firewall deployment was the source of this alert.

View all of the supporting observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend:

Procedure

Step 1 From the alert detail, click the arrow icon (➔) next to an observation type to view all logged observations of that type.

Step 2 Click the arrow icon (➔) next to **All Observations for Network** to view all logged observations for this alert's source entity.

Download the supporting observations in a comma-separated value file, if you want to perform additional analysis on these observations:

- From the alert detail, in the Supporting Observations pane, click **CSV**.

From the observations, determine if the source entity behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.

View additional context surrounding the source entity from a source entity IP address or hostname, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting:

- Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
- Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
- Select **Device** from the IP address or hostname drop-down to view information about the device.
- Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that the source entity in Secure Cloud Analytics is always internal to your network. Contrast this with the Initiator IP in a firewall event, which indicates the entity that initiated a connection, and may be internal or external to your network.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

Review the context for an external entity IP address or hostname with which the source entity established a connection:

- Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
- Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
- Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
- Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
- Select **Talos Intelligence** from the IP address or hostname drop-down to view information about this information on Talos's website.
- Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
- Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that connected entities in Secure Cloud Analytics are always external to your network. Contrast this with the Responder IP in a firewall event, which indicates the entity that responded to a connection request, and may be internal or external to your network.

Leave comments as to your findings.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Examine the entity and users

After you review the alert in the Secure Cloud Analytics portal UI, you can perform an additional examination on a source entity directly, any users that may have been involved with this alert, and other related entities.

- Determine where the source entity is on your network, physically or in the cloud, and access it directly. Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.

- Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.
- Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.

Leave comments as to your findings:

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Remediate issues using Secure Cloud Analytics

If malicious behavior caused the alert, remediate the malicious behavior. For example:

- If a malicious entity or user attempted to log in from outside your network, update your firewall rules and firewall configuration to prevent the entity or user from accessing your network.
- If an entity attempted to access an unauthorized or malicious domain, examine the affected entity to determine if malware is the cause. If there are malicious DNS redirects, determine if other entities on your network are affected, or part of a botnet. If this is intended by a user, determine if there is a legitimate reason for this, such as testing firewall settings. Update your firewall rules and firewall configuration to prevent further access to the domain.
- If an entity is exhibiting behavior that is different from the historical entity model behavior, determine if the behavior change is intended. If it is unintended, examine whether an otherwise authorized user on your network is responsible for the change. Update your firewall rules and firewall configuration to address unintended behavior if it involves connections with entities that are external to your network.
- If you identify a vulnerability or exploit, update or patch the affected entity to remove the vulnerability, or update your firewall configuration to prevent unauthorized access. Determine if other entities on your network may similarly be affected, and apply the same update or patch to those entities. If the vulnerability or exploit currently does not have a fix, contact the appropriate vendor to let them know.
- If you identify malware, quarantine the entity and remove the malware. Review the firewall file and malware events to determine if other entities on your network are at risk, and quarantine and update the entities to prevent this malware from spreading. Update your security intelligence with information about this malware, or the entities that caused this malware. Update your firewall access control and file and malware rules to prevent this malware from infecting your network in the future. Alert vendors as necessary.
- If malicious behavior resulted in data exfiltration, determine the nature of the data sent to an unauthorized source. Follow your organization's protocols for unauthorized data exfiltration. Update your firewall configuration to prevent future data exfiltration attempts by this source.

Update and close the alert

Add additional tags based on your findings:

Procedure

Step 1 In the Secure Cloud Analytics portal UI, select **Monitor** > **Alerts**.

Step 2 Select one or more **Tags** from the drop-down.

Add final comments describing the results of your investigation, and any remediation steps taken:

- From an alert's detail, enter a **Comment on this alert**, then click **Comment**.

Close the alert, and mark it as helpful or not helpful:

1. From an alert's detail, click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. Note that this does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. Click **Save**.

What to do next

Reopen a closed alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

Reopen a closed alert:

- From a closed alert's detail, click **Reopen Alert**.

Modifying Alert Priorities

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to *low* or *normal* priority, based on Cisco intelligence and other factors. Based on your network environment, you may want to reprioritize alert types, to emphasize certain alerts that you are concerned with. You can configure any alert type to be *low*, *normal*, or *high* priority.

- Select **Monitor** > **Alerts**.
- Click the settings drop-down icon (), then select **Alert Types and Priorities**.
- Click the edit icon () next to an alert type and select *low*, *medium*, or *high* to change the priority.

Viewing Live Events

The Live events page shows the most recent 500 events that match the Searching for and Filtering Events in the Event Logging Page you entered. If the Live events page displays the maximum of 500 events, and more events stream in, Security Cloud Control displays the newest live events, and transfers the oldest live events to the Historical events page, keeping the total number of live events at 500. That transfer takes roughly a minute to perform. If no filtering criteria is added, you will see all the latest Live 500 events generated by rules configured to log events.

The event timestamps are shown in UTC.

Changing the filtering criteria, whether live events are playing or paused, clears the events screen and restarts the collection process.

To see live events in the Security Cloud Control Events viewer:

Procedure

Step 1 In the left pane, choose **Events & Logs** > **Events**.

Step 2 Click the **Live** tab.

What to do next

See how to play and pause events by reading .

Related Information:

- Play/Pause Live Events, on page 660
- View Historical Events, on page 661
- Customize the Events View, on page 662

Play/Pause Live Events

You can "play" or "pause" live events as they stream in. If live events are "playing," Security Cloud Control displays events that match the filtering criteria specified in the Events viewer in the order they are received. If events are paused, Security Cloud Control does not update the Live events page until you restart playing live events. When you restart playing events, Security Cloud Control begins populating events in the Live page from the point at which you restarted playing events. It doesn't back-fill the ones you missed.

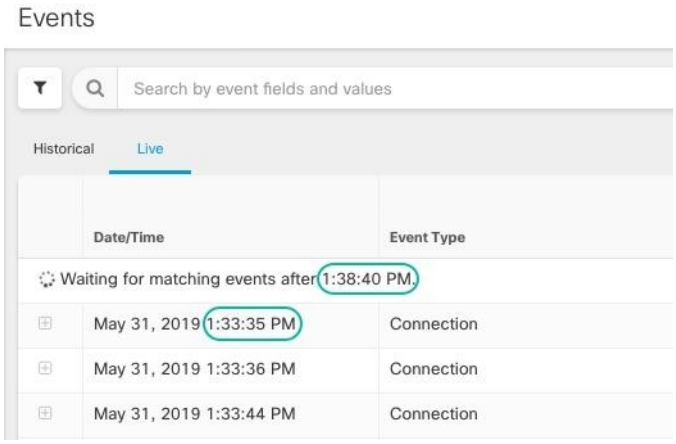
To view all the events that Security Cloud Control received whether you played or paused live event streaming, click the **Historical** tab.

Auto-pause Live Events

After displaying events for about 5 consecutive minutes, Security Cloud Control warns you that it is about to pause the stream of live events. At that time, you can click the link to continue streaming live events for another 5 minutes or allow the stream to stop. You can restart the live events stream when you are ready.

Receiving and Reporting Events

There may be a small lag between the Secure Event Connector (SEC) receiving events and Security Cloud Control posting events in the Live events viewer. You can view the gap on the Live page. The time stamp of the event is the time it was received by SEC.



View Historical Events

The Live events page shows the most recent 500 events that match the Searching for and Filtering Events in the Event Logging Page you entered. Events older than the most recent 500 are transferred to the Historical events table. That transfer takes roughly a minute to perform. You can then filter all the events you have stored to find events you're looking for.

To view historical events:

Procedure

Step 1 In the navigation pane, choose **Events & Logs** > **Events**.

Step 2 Click the **Historical** tab. By default, when you open the Historical events table, the filter is set to display the events collected within the last hour.

The event attributes are largely the same as what is reported by Firepower Device Manager (FDM) or the Adaptive Security Device Manager (ASDM).

- For a complete description of Firepower Threat Defense event attributes, see Cisco FTD Syslog Messages.
- For a complete description of ASA event attributes, see Cisco ASA Series Syslog Messages.

Customize the Events View

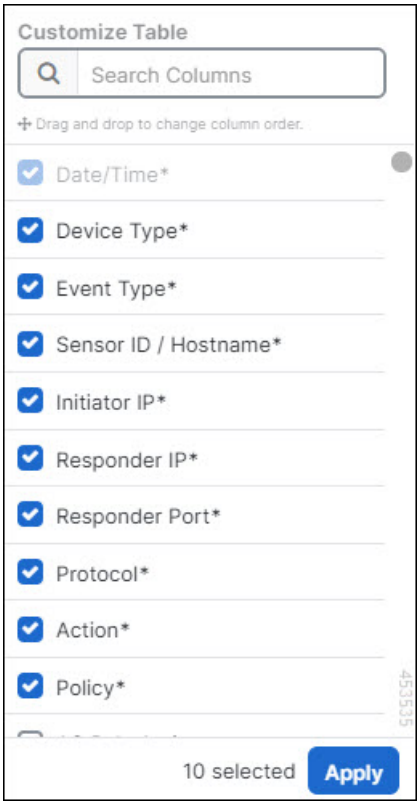
Any changes made to the Event Logging page are automatically saved for when you navigate away from this page and come back at a later time.

Note The Live and Historical events view have the same configuration. When you customize the events view, these changes are applied to both the Live and Historical view.

Show or Hide Columns

You can modify the event view for both live and historical events to only include column headers that apply to the view you want. Click the column filter icon located to the right of the columns, select or deselect the columns you want, and then click **Apply**.

Figure 9: Show or Hide Columns



Columns with asterisks are provided within the event table by default, although you can remove them at any time.

Search and Add Columns

You can search for more columns, which are not part of the default list, and add them to the event view for both live and historical events. Note that adding many columns for customizing the table may reduce performance. Consider using fewer columns for faster data retrieval.

Alternatively, click the + icon next to an event to expand it and view the hidden columns. Note that some of the event fields displayed when you expand an event can have a different name compared to the corresponding column name. To correlate the events fields displayed when you expand an event to the corresponding column name, see Correlate Threat Defense Event Fields and Column Names.

Reorder the Columns

You can reorder the columns of the event table. Click the column filter icon  located to the right of the columns to view the list of selected columns. Then, drag and drop the columns into the order you want. The column at the top of the list in the drop-down menu appears as the left-most column in the event table.

Related Information:

- Searching for and Filtering Events in the Event Logging Page
- Event Attributes in Security Analytics and Logging

Correlate Threat Defense Event Fields and Column Names

On the Security Cloud Control **Event Logging** page, you can click on any event to expand its details and view all the associated event fields. Note that the names of some event fields may differ from those of the column headers in the Security Cloud Control event viewer where the values of these fields are displayed. The table below lists those threat defense event fields that have differing column names and provides a comparison between the threat defense event field and the respective column name.

Table 17: Threat Defense Event Field and the Corresponding Security Cloud Control Column Name

Security Cloud Control Column Name	FTD Event Field
Date/Time	Timestamp
Detection Type	ClientAppDetector
Encrypted Visibility Fingerprint	EVE_Fingerprint
Encrypted Visibility Process Name	EVE_Process
Encrypted Visibility Process Confidence Score	EVE_ProcessConfidencePct
Encrypted Visibility Threat Confidence	EVE_ThreatConfidenceIndex
Encrypted Visibility Threat Confidence Score	EVE_ThreatConfidencePct
MITRE	MitreAttackGroups
NAT Source IP	NAT_InitiatorIP
NAT Source Port	NAT_InitiatorPort

Security Cloud Control Column Name	FTD Event Field
Rule Group	SnortRuleGroups

Show and Hide Columns on the Event Logging Page

The Event Logging page displays ASA and FTD syslog events and ASA NetFlow Secure Event Logging (NSEL) events sent to the Cisco cloud from configured ASA and FDM-managed devices.

You can show or hide columns on the Event Logging page by using the Show/Hide widget with the table:

Procedure

Step 1 In the left pane, choose **Events & Logs** > **Events** .

Step 2 Scroll to the far right of the table and click the column filter icon ≡.

Step 3 Check the columns you want to see and uncheck the columns you want to hide.

Other users logging into the tenant will see the same columns you chose to show until columns are shown or hidden again.

This table describes the default column headers:

Column Header	Description
Date/Time	The time the device generated the event. By default, event timestamps are displayed in your Local time zone. To view event timestamps in UTC, see Change the Time Zone for the Event Timestamps, on page 666
Device Type	FTD (Firepower Threat Defense)

Column Header	Description

Event Type	This composite column can have any of the following:
	• **FTD Event Types**
	  • Connection: Displays connection events from access control rules.
	  • File: Displays events reported by file policies in access control rules.
	  • Intrusion: Displays events reported by intrusion policy in access control rules.
	  • Malware: Displays events reported by malware policies in access control rules.
	• ASA **Event Types**: These event types represent groups of syslog or NetFlow events. See ASA Event Types for more information about which syslog ID or which NetFlow ID is included in which group.
	  • Parsed Events: Parsed syslog events contain more event attributes than other syslog events and Security Cloud Control is able to return search results based on those attributes more quickly. Parsed events are not a filtering category; however, parsed event IDs are displayed in the Event Types column in *italics*. Event IDs that are not displayed in italics are not parsed.
	  • ASA NetFlow Event IDs: All Netflow (NSEL) events from ASA appear here.

Sensor ID	The Sensor ID is the IP address from which events are sent to the Secure Event Connector. This is typically the Management interface on the Firepower Threat Defense or the ASA.
Initiator IP	This is the IP address of the source of the network traffic. The value of the Initiator address field corresponds to the value of the InitiatorIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.

Column Header	Description
Responder IP	This is the destination IP address of the packet. The value of the Destination address field corresponds to the value in the ResponderIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.
Port	The port or ICMP code used by the session **responder**. The value of the destination port corresponds to the value of the **ResponderPort** in the event details.
Protocol	It represents the protocol in the events.
Action	Specifies the security action defined by the rule. The value you enter must be an exact match to what you want to find; however, the case doesn't matter. Enter different values for connection, file, intrusion, malware, syslog, and NetFlow event types: • For connection event types, the filter searches for matches in the AC_RuleAction attribute. Those values could be Allow, Block, Trust. • For file event types, the filter searches for matches in the FileAction attribute. Those values could be Allow, Block, Trust. • For intrusion event types, the filter searches for matches in the InLineResult attribute. Those values could be Allowed, Blocked, Trusted. • For malware event types, the filter searches for matches in the FileAction attribute. Those values could be Cloud Lookup Timeout. • For syslog and NetFlow events types, the filter searches for matches in the Action attribute.
Policy	The name of the policy that triggered the event. Names will be different for ASA and FDM-managed devices.

Related Information:

Searching for and Filtering Events in the Event Logging Page, on page 698

Change the Time Zone for the Event Timestamps

Change the time zone display for event timestamps on the Security Cloud Control **Event Logging** page.

Procedure

Step 1 From the left pane, choose **Events & Logs** > **Events**.

Step 2 Click the **UTC Time** or **Local Time** button on the top right side of the **Event Logging** page to display the event timestamps in the selected time zone.

By default, event timestamps are displayed in your local time zone.

Customizable Event Filters

If you are a Secure Logging Analytics (SaaS) customer, you can create and save custom filters that you use frequently.

The elements of your filter are saved to a filter tab as you configure them. Whenever you return to the Event Logging page, these searches will be available to you. They will not be available to other Security Cloud Control users of the tenant. They will not be available to you on a different tenant, if you manage more than one tenant.

Note Be aware that when you are working in a filter tab, if you modify any filter criteria, those changes are saved to your custom filter tab automatically.

Procedure

Step 1 From the main menu, choose **Events & Logs** > **Events**.

Step 2 Clear the Search field of any values.

Step 3 Above the event table, click the blue plus button to add a View tab. Filter views are labeled "View 1", "View 2", "View 3" and so on until you give them a name.

Step 4 Select a view tab.

Step 5 Open the filter bar and select the filters attributes you want in your custom filter. See Searching for and Filtering Events in the Event Logging Page, on page 698. Remember that only filter attributes are saved in the custom filter.

Step 6 Customize the columns you want to show in the event logging table. See Show and Hide Columns on the Event Logging Page, on page 664 for a discussion of showing and hiding columns.

Step 7 Double-click the filter tab with the "View X" label and rename it.

Step 8 (Optional) Now that you have created a custom filter, you can fine tune the results displayed on the Event Logging page, without changing the custom filter, by adding search criteria to the Search field. See Searching for and Filtering Events in the Event Logging Page, on page 698.

Event Attributes in Security Analytics and Logging

Event Attribute Descriptions

The event attribute descriptions used by Security Cloud Control are largely the same as what is reported by Firepower Device Manager (FDM) and Adaptive Security Device Manager (ASDM).

- For a complete description of FDM-managed device event attributes, see Cisco Firepower Threat Defense Syslog Messages.

Some ASA syslog events are "parsed" and others have additional attributes which you can use when filtering the contents of the Event Logging table using attribute:value pairs. See these additional topics for other important attributes of syslog events:

- EventGroup and EventGroupDefinition Attributes for Some Syslog Messages
- EventName Attributes for Syslog Events
- Time Attributes in a Syslog Event

EventGroup and EventGroupDefinition Attributes for Some Syslog Messages

Some syslog events will have the additional attributes "EventGroup" and "EventGroupDefinition". You will be able to filter the events table to find events using these additional attributes by filtering by attribute:value pairs. For example, you could filter for Application Firewall events by entering `apfw:415*` in the search field of the Event Logging table.

Syslog Message Classes and Associated Message ID Numbers

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
aaa/auth	User Authentication	109, 113
acl/session	Access Lists/User Session	106
apfw	Application Firewall	415
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
citrix	Citrix Client	723
clst	Clustering	747
cmgr	Card Management	323
config	Command Interface	111, 112, 208, 308

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policies	734
eap, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
eigrp	EIGRP Routing	336
email	E-mail Proxy	719
ipaa/envmon	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
idfw	Identity-based Firewall	746
ids	Intrusion Detection System	733
ids/ips	Intrusion Detection System / Intrusion Protection System	400
ikev2	IKEv2 Toolkit	750, 751, 752
ip	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	401, 420
ipv6	IPv6	325
l4tm	Block lists, Allow lists, grey lists	338
lic	Licensing	444
mdm-proxy	MDM Proxy	802
nac	Network Admission Control	731, 732
vpn/nap	IKE and IPsec / Network Access Point	713
np	Network Processor	319
ospf	OSPF Routing	318, 409, 503, 613
passwd	Password Encryption	742
pp	Phone Proxy	337
rip	RIP Routing	107, 312
rm	Resource Manager	321
sch	Smart Call Home	120

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
session	User Session	108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
session/natpat	User Session/NAT and PAT	305
snmp	SNMP	212
ssafe	ScanSafe	775
ssl/np ssl	SSL Stack/NP SSL	725
svc	SSL VPN Client	722
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741
tre	Transactional Rule Engine	780
ucime	UC-IME	339
tag-switching	Service Tag Switching	779
td	Threat Detection	733
vm	VLAN Mapping	730
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
vxlan	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and AnyConnect Client	716
session/natpat	User Session / NAT and PAT	305

EventName Attributes for Syslog Events

Some syslog events will have the additional attribute "EventName". You will be able to filter the events table to find events using the EventName attribute by filtering by attribute:value pairs. For example, you could filter events for a "Denied IP packet" by entering **EventName:"Denied IP Packet"** in the search field of the Event Logging table.

Syslog Event ID and Event Names Tables

- AAA Syslog Event IDs and Event Names

- Botnet Syslog Event IDs and Event Names
- Failover Syslog Event IDs and Event Names
- Firewall Denied Syslog Event IDs and Event Names
- Firewall Traffic Syslog Event IDs and Event Names
- Identity Based Firewall Syslog Event IDs and Event Names
- IPSec Syslog Event IDs and Event Names
- NAT Syslog Event ID and Event Names
- SSL VPN Syslog Event IDs and Event Names

AAA Syslog Event IDs and Event Names

EventID	EventName
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	Authentication Failed
109007	Authorization Success
109008	Authorization Failed
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached

EventID	EventName
109023	AAA auth required
109024	Authorization Failed
109025	Authorization Failed
109026	AAA error
109027	AAA Server error
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	Authentication Failed
109032	AAA ACL error
109033	Authentication Failed
109034	Authentication Failed
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved
113012	Authentication Successful
113013	AAA error
113014	AAA error
113015	Authentication Rejected
113016	AAA Rejected

EventID	EventName
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

Botnet Syslog Event IDs and Event Names

EventID	EventName
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed

EventID	EventName
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

Failover Syslog Event IDs and Event Names

EventID	EventName
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error

EventID	EventName
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

Firewall Denied Syslog Event IDs and Event Names

EventID	EventName
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy

EventID	EventName
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

Firewall Traffic Syslog Event IDs and Event Names

EventID	EventName
108001	Inspect SMTP
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found

EventID	EventName
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP

EventID	EventName
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	Memory Error
324003	GTP Pkt Drop
324004	GTP Version Not Supported
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp

EventID	EventName
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	IPS ICMP Information Request
400020	IPS ICMP Information Reply
400021	IPS ICMP Address Mask Request
400022	IPS ICMP Address Mask Reply
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack

EventID	EventName
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type

EventID	EventName
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied Packet
424002	Dropped Packet
431001	Dropped RTP
431002	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header

EventID	EventName
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

Identity Based Firewall Syslog Event IDs and Event Names

EventID	EventName
746001	Import started
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped

EventID	EventName
746010	Import user failed
746011	Exceed user limit
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec Syslog Event IDs and Event Names

EventID	EventName
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure
402121	Packet dropped
426101	cLACP Port Bundle
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT Syslog Event ID and Event Names

EventID	EventName
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	Connection Limit exceeded
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN Syslog Event IDs and Event Names

EventID	EventName
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled

EventID	EventName
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful

EventID	EventName
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message

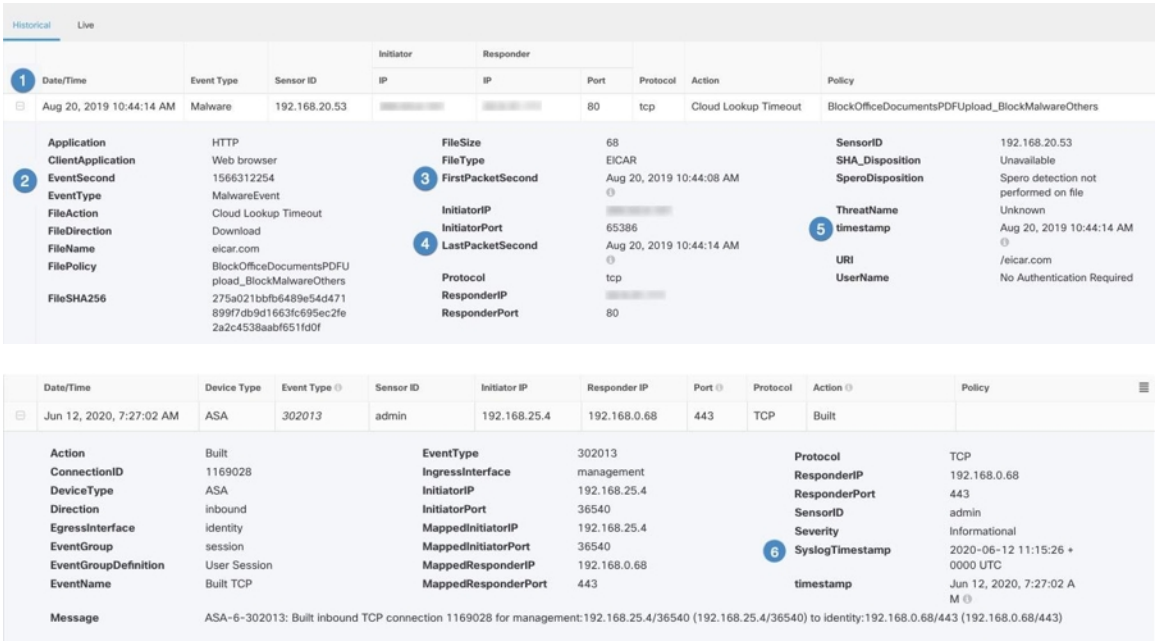
EventID	EventName
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol

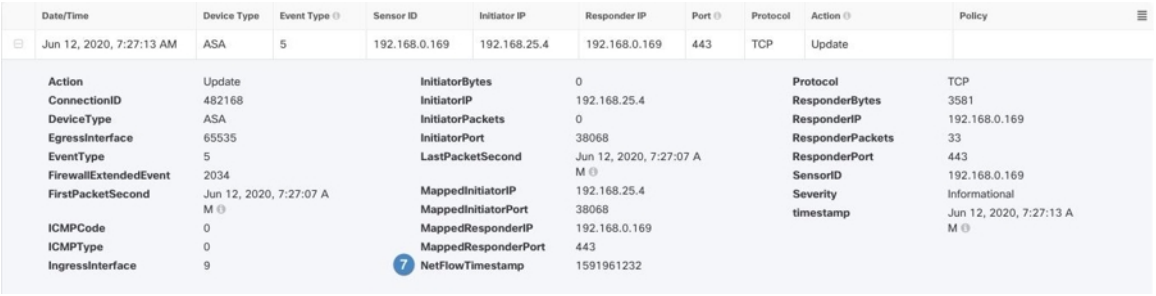
EventID	EventName
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication

EventID	EventName
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014	SSL LIB error
725015	SSL client certificate failed

Time Attributes in a Syslog Event

Understanding the purposes of the different time-stamps in the Event Logging page will help you filter and find the events that interest you.





Number	Label	Description
1	Date/Time	The time the Secure Event Connector (SEC) processed the event. This may not be the same as the time the firewall inspected that traffic. Same value as timestamp.
2	EventSecond	Equals with LastPacketSecond.
3	FirstPacketSecond	The time at which the connection opened. The firewall inspects the packet at this time. The value of the FirstPacketSecond is calculated by subtracting the ConnectionDuration from the LastPacketSecond. For connection events logged at the beginning of the connection, the value of FirstPacketSecond, LastPacketSecond, and EventSecond will all be the same.
4	LastPacketSecond	The time at which the connection closed. For connection events logged at the end of the connection, LastPacketSecond and EventSecond will be equal.
5	timestamp	The time the Secure Event Connector (SEC) processed the event. This may not be the same as the time the firewall inspected that traffic. Same value as Date/Time.
6	Syslog TimeStamp	Represents the syslog originated time if 'logging timestamp' is used. If the syslog does not have this info, the time the SEC received the event is reflected.

Number	Label	Description
7	NetflowTimeStamp	The time at which the ASA finished gathering enough flow records/events to fill a NetFlow packet to then send them off to a flow collector.

Cisco Secure Cloud Analytics and Dynamic Entity Modeling

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Secure Cloud Analytics is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Dynamic Entity Modeling

Dynamic entity modeling tracks the state of your network by performing a behavioral analysis on firewall events and network flow data. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they take on your network. Secure Cloud Analytics, integrated with a **Logging Analytics and Detection** license, can draw from firewall events and other traffic information in order to determine the types of traffic the entity usually transmits. If you purchase a **Total Network Analytics and Monitoring** license, Secure Cloud Analytics can also include NetFlow and other traffic information in modeling entity traffic. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity. From this information, Secure Cloud Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, or a remote access session established with another entity. If you integrate with Security Cloud Control, these facts can be obtained from firewall events. If you also purchase a **Total Network Analytics and Monitoring**, license, the system can also obtain facts from NetFlow, and generate observations from both firewall events and NetFlow. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Alerts and Analysis

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system. Note

that one alert may represent multiple observations. If a firewall logs multiple connection events related to the same connection and entities, this may result in only one alert.

For example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

Note that when you view and close alerts in Secure Cloud Analytics, you cannot allow or block traffic from the Secure Cloud Analytics UI. You must update your firewall access control rules to allow or block traffic, if you deployed your devices in active mode, or your firewall access control rules if your firewalls are deployed in passive mode.

Working with Alerts Based on Firewall Events

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alerts Workflow

An alert's workflow is based around its status. When the system generates an alert, the default status is Open, and no user is assigned. When you view the Alerts summary, all open alerts are displayed by default, as these are of immediate concern.

Note: If you have a **Total Network Analytics and Monitoring** license, your alerts can be based on observations generated from NetFlow, observations generated from firewall events, or observations from both data sources.

As you review the Alerts summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees. You can set an alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert, to display it as an open alert again. As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert. This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior.

As you research within the Secure Cloud Analytics web portal UI, in Security Cloud Control, and on your network, you can leave comments with the alert that describe your findings. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed, and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

The following presents general guidelines and suggestions for how to investigate a given alert. Because Secure Cloud Analytics provides additional context when it logs an alert, you can use this context to help guide your investigation.

These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

In general, you can take the following steps when you review an alert:

1. Triage open alerts, on page 654
2. Snooze alerts for later analysis, on page 655
3. Update the alert for further investigation, on page 655
4. Review the alert and start your investigation, on page 656
5. Examine the entity and users, on page 657
6. Remediate issues using Secure Cloud Analytics, on page 658
7. Update and close the alert, on page 658

Triage open alerts

Triage the open alerts, especially if more than one have yet to be investigated:

- See Viewing Cisco Secure Cloud Analytics Alerts from Security Cloud Control for more information on cross-launching from Security Cloud Control to Secure Cloud Analytics, and viewing alerts.

Ask the following questions:

- Have you configured this alert type as high priority?
- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?
- If there is communication with external entities, have these entities established connections with other entities on your network in the past?

If this is a *high* priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

Snooze alerts for later analysis

Snooze alerts when they are of lesser priority, as compared to other alerts. For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert (indicating that an entity's current traffic matches a behavior profile that it did not previously match), you can snooze this

alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

Snooze an alert:

Procedure

Step 1 Click **Close Alert**.

Step 2 In the Snooze this alert pane, select a snooze period from the drop-down.

Step 3 Click **Save**.

What to do next

When you are ready to review these alerts, you can unsnooze them. This sets the status to Open, and displays the alert alongside the other Open alerts.

Unsnooze a snoozed alert:

- From a snoozed alert, click **Unsnooze Alert**.

Update the alert for further investigation

Open the alert detail:

Procedure

Step 1 Select **Monitor** > **Alerts**.

Step 2 Click an alert type name.

What to do next

Based on your initial triage and prioritization, assign the alert and tag it:

1. Select a user from the **Assignee** drop-down to assign the alert, so a user can start investigating.
2. Select one or more **Tags** from the drop-down to add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.
3. Enter a **Comment on this alert**, then click **Comment** to leave comments as necessary to track your initial findings, and assist the person assigned to the alert. The alert tracks both system comments and user comments.

Review the alert and start your investigation

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert. Review the supporting observations to understand what these observations mean for the source entity.

Note that if the alert was generated based on firewall events, the system does not note that your firewall deployment was the source of this alert.

View all of the supporting observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend:

Procedure

Step 1 From the alert detail, click the arrow icon (➔) next to an observation type to view all logged observations of that type.

Step 2 Click the arrow icon (➔) next to **All Observations for Network** to view all logged observations for this alert's source entity.

Download the supporting observations in a comma-separated value file, if you want to perform additional analysis on these observations:

- From the alert detail, in the Supporting Observations pane, click **CSV**.

From the observations, determine if the source entity behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.

View additional context surrounding the source entity from a source entity IP address or hostname, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting:

- Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
- Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
- Select **Device** from the IP address or hostname drop-down to view information about the device.
- Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that the source entity in Secure Cloud Analytics is always internal to your network. Contrast this with the Initiator IP in a firewall event, which indicates the entity that initiated a connection, and may be internal or external to your network.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity

established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

Review the context for an external entity IP address or hostname with which the source entity established a connection:

- Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
- Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
- Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
- Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
- Select **Talos Intelligence** from the IP address or hostname drop-down to view information about this information on Talos's website.
- Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
- Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that connected entities in Secure Cloud Analytics are always external to your network. Contrast this with the Responder IP in a firewall event, which indicates the entity that responded to a connection request, and may be internal or external to your network.

Leave comments as to your findings.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Examine the entity and users

After you review the alert in the Secure Cloud Analytics portal UI, you can perform an additional examination on a source entity directly, any users that may have been involved with this alert, and other related entities.

- Determine where the source entity is on your network, physically or in the cloud, and access it directly. Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.
- Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.
- Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.

Leave comments as to your findings:

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Update and close the alert

Add additional tags based on your findings:

Procedure

Step 1 In the Secure Cloud Analytics portal UI, select **Monitor** > **Alerts**.

Step 2 Select one or more **Tags** from the drop-down.

Add final comments describing the results of your investigation, and any remediation steps taken:

- From an alert's detail, enter a **Comment on this alert**, then click **Comment**.

Close the alert, and mark it as helpful or not helpful:

1. From an alert's detail, click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. Note that this does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. Click **Save**.

What to do next

Reopen a closed alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

Reopen a closed alert:

- From a closed alert's detail, click **Reopen Alert**.

Modifying Alert Priorities

Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to *low* or *normal* priority, based on Cisco intelligence and other factors. Based on your network environment, you may want to reprioritize alert types, to emphasize certain alerts that you are concerned with. You can configure any alert type to be *low*, *normal*, or *high* priority.

- Select **Monitor** > **Alerts**.
- Click the settings drop-down icon (), then select **Alert Types and Priorities**.
- Click the edit icon () next to an alert type and select *low*, *medium*, or *high* to change the priority.

Searching for and Filtering Events in the Event Logging Page

Searching and filtering the historical and live event tables for specific events, works the same way as it does when searching and filtering for other information in Security Cloud Control. As you add filter criteria, Security Cloud Control starts to limit what it displays on the **Event Logging** page. You can also enter search criteria in the search field to find events with specific values. If you combine the filtering and searching mechanisms, search tries to find the value you entered from among the results displayed after filtering the events.

Following are the options to conduct a search for event logs:

- Search for Events in the Events Logging Page, on page 705
- Search Historical Events in the Background, on page 704

Filtering works the same way for live events as it does for historical events with the exception that live events cannot be filtered by time.

Learn about these filtering methods:

- Filter Live or Historical Events, on page 698
- Filter Only NetFlow Events, on page 700
- Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events, on page 700
- Combine Filter Elements, on page 700

Filter Live or Historical Events

This procedure explains how to use event filtering to see a subset of events in the Event Logging page. If you find yourself repeatedly using certain filter criteria, you can create a customized filter and save it. See Customizable Event Filters for more information.

Procedure

Step 1 In the navigation bar, choose **Events & Logs** > **Events**

Step 2 Click either the **Historical** or **Live** tab.

Step 3 Click the filter button . Click the pin icon to pin the **Filter** pane and keep it open.

Step 4 Click a view tab that has no saved filter elements.

Step 5 Select the event details you want to filter by:

- **FTD Events**
  - Connection: Displays connection events from access control rules.
  - File: Displays events reported by file policies in access control rules.
  - Intrusion: Displays events reported by intrusion policy in access control rules.

- Malware: Displays events reported by malware policies in access control rules.

- **ASA Events**: These event types represent groups of syslog or NetFlow events.

  See Event Types in Security Cloud Control for more information about events.

- **Time Range**: Click the Start or End time fields to select the beginning and end of the time period you want to display. The time stamp is displayed in the local time of your computer.

- **Action**: Specifies the security action defined by the rule. The value you enter must be an exact match to what you want to find; however, the case doesn't matter. Enter different values for connection, file, intrusion, malware, syslog, and NetFlow event types:

  - For connection event types, the filter searches for matches in the AC_RuleAction attribute. Those values could be Allow, Block, Trust.
  - For file event types, the filter searches for matches in the FileAction attribute. Those values could be Allow, Block, Trust.
  - For intrusion event types, the filter searches for matches in the InLineResult attribute. Those values could be Allowed, Blocked, Trusted.
  - For malware event types, the filter searches for matches in the FileAction attribute. Those values could be Cloud Lookup Timeout.
  - For syslog and NetFlow events types, the filter searches for matches in the Action attribute.

- **Sensor ID**: The Sensor ID is the the Management IP address from which events are sent to the Secure Event Connector.

  For an FDM-managed device, the Sensor ID is typically the IP address of the device's management interface.

- **IP addresses**

  - **Initiator** : This is the IP address of the source of the network traffic. The value of the Initiator address field corresponds to the value of the InitiatorIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.
  - **Responder**: This is the destination IP address of the packet. The value of the Destination address field corresponds to the value in the ResponderIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.

- **Ports**

  - **Initiator**: The port or ICMP type used by the session initiator. The value of the source port corresponds to the value fo the InitiatorPort in the event details. (Add a range - starting port ending port and space in between or both initiator and responder)
  - **Reponder**: The port or ICMP code used by the session responder. The value of the destination port corresponds to the value of the ResponderPort in the event details.

Step 6 (Optional) Save your filter as a custom filter by clicking out of the view tab.

Filter Only NetFlow Events

This procedure finds only ASA NetFlow events:

Procedure

Step 1 From the left menu, choose **Events & Logs** > **Events**.

Step 2 Click the Filter icon and pin the filter open.

Step 3 Check **Netflow** ASA Event filter.

Step 4 Clear all other ASA Event filters.

Only ASA NetFlow events are displayed in the Event Logging table.

Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events

This procedure finds only syslog events:

Procedure

Step 1 In the left pane, choose **Events & Logs** > **Events**.

Step 2 Click the Filter icon and pin the filter open.

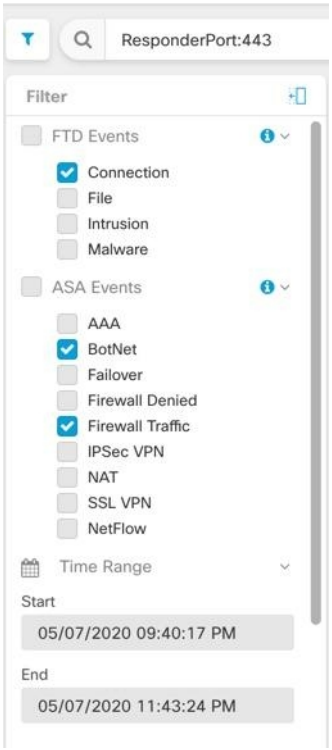
Step 3 Scroll to the bottom of the **Filter** pane and make sure the **Include NetFlow events** filter is **unchecked**.

Step 4 Scroll back up to the ASA Events filter tree, and make sure the **NetFlow** box is **unchecked**.

Step 5 Select the rest of your ASA or FTD filter criteria.

Combine Filter Elements

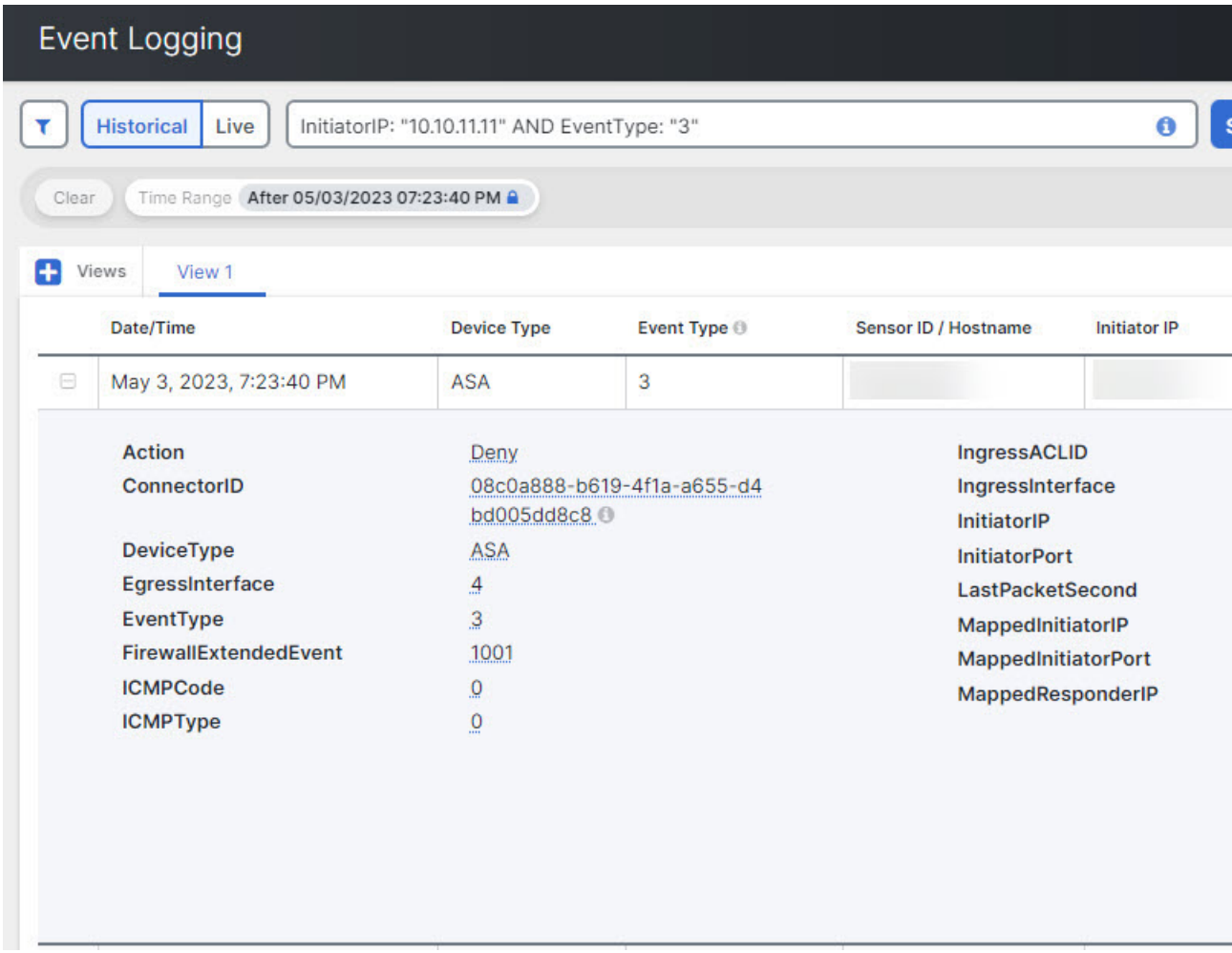
Filtering events generally follows the standard filtering rules in Security Cloud Control: The filtering categories are "AND-ed" and the values within the categories are "OR-ed." You can also combine the filter with your own search criteria. In the case of event filters; however, the device event filters are also "OR-ed." For example, if these values were chosen in the filter:



With this filter in use, Security Cloud Control would display threat defense device connection events **or** ASA BotNet **or** Firewall Traffic events, **and** those events that occurred between the two times in the time range, **and** those events that also contain the ResponderPort 443. You can filter by historical events within a time range. The live events page always displays the most recent events.

Search for Specific Attribute: Value Pairs

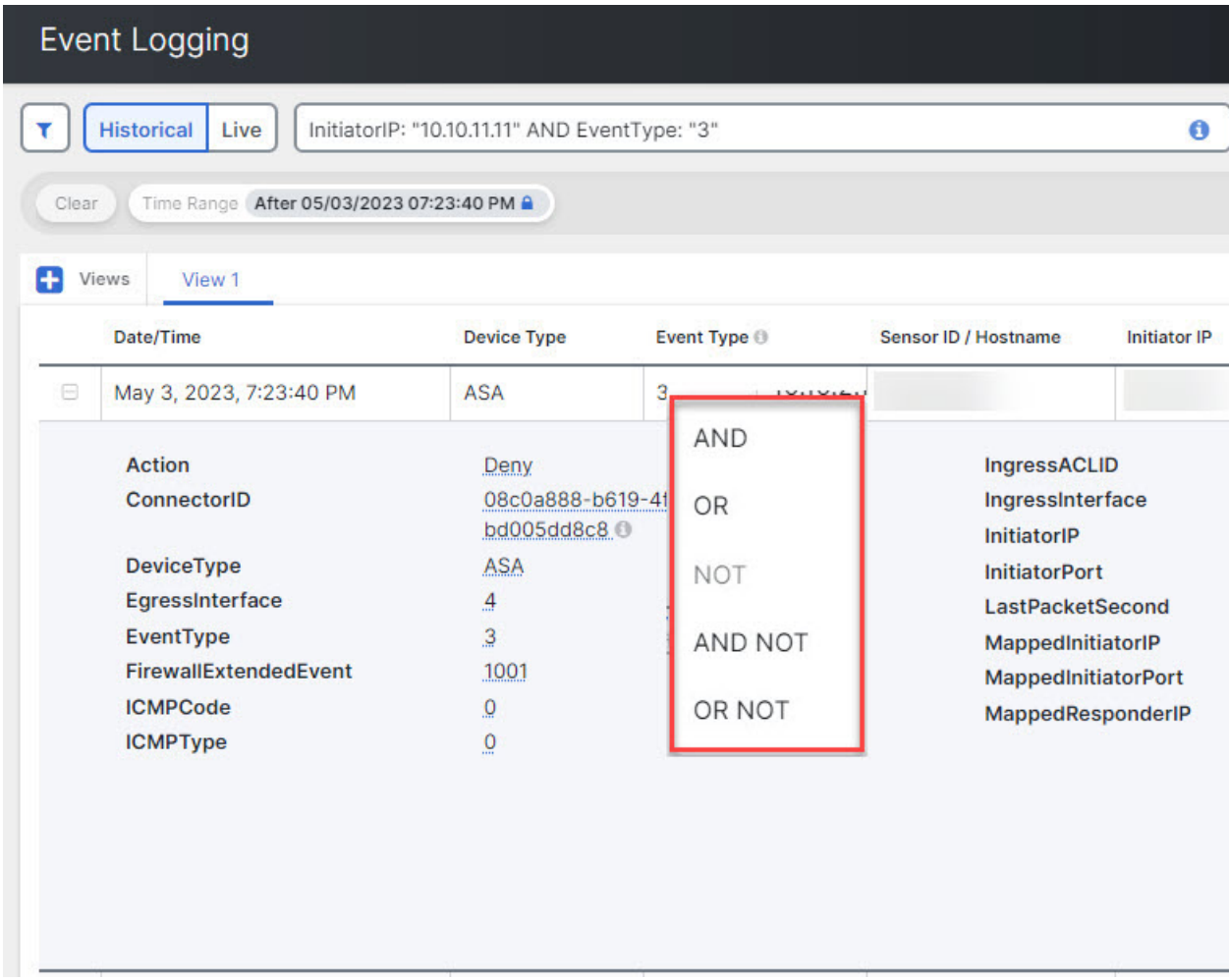
You can search for live or historical events by entering an event attribute and a value in the search field. The easiest way to do this is to click the attribute in the Event Logging table that you want to search for, and Security Cloud Control enters it in the Search field. The events you can click on will be blue when you roll over them. Here is an example:



In this example, the search started by rolling over the InitiatorIP value of 10.10.11.11 and clicking it. Initiator IP and it's value were added to the search string. Next, Event Type, 3 was rolled-over and clicked and added to the search string and an AND was added by Security Cloud Control. So the result of this search will be a list of events that were initiated from 10.10.11.11 AND that are 3 event types.

Notice the magnifying glass next to the value 3 in the example above. If you roll-over the magnifying glass, you could also choose an AND, OR, AND NOT, OR NOT operator to go with the value you want to add to the search.

In the example below, "OR" is chosen. The result of this search will be a list of events that were initiated from 10.10.11.11 OR are a 106023 event type. Note that if the search field is empty and you right click a value from the table, only NOT is available as there is no other value.



As long as you rollover a value and it is highlighted blue, you can add that value to the search string.

AND, OR, NOT, AND NOT, OR NOT Filter Operators

Here are the behaviors of "AND", "OR", "NOT", "AND NOT", and "OR NOT" used in a search string:

AND

Use the AND operator in the filter string, to find events that include all attributes. The AND operator cannot begin a search string.

For example, the search string below will search for events that contain the TCP protocol AND that originated from InitiatorIP address 10.10.10.43, AND that were sent from the Initiator port 59614. One would expect that with each additional AND statement, the number of events that meet the criteria would be small and smaller.

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

OR

Use the OR operator in the filter string, to find events that include any of the attributes. The OR operator cannot begin a search string.

For example, the search string below will display events in the event viewer that include events that include the TCP protocol, OR that originated from InitiatorIP address 10.10.10.43, OR that were sent from the Initiator port 59614. One would expect that with each additional OR statement, the number of events that meet the criteria would be bigger and bigger.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT

Use this only at the beginning of a search string to exclude events with certain attribtues. For example, this search string would exclude any event with the InitiatorIP 192.168.25.3 from the results.

```
NOT InitiatorIP: "192.168.25.3"
```

AND NOT

Use the AND NOT operator in the filter string to exclude events that contain certain attributes. AND NOT cannot be used at the beginning of a search string.

For example, this filter string will display events with the InitiatorIP 192.168.25.3 but not those whose ResponderIP address is also 10.10.10.1.

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

You can also combine NOT and AND NOT to exclude several attributes. For example this filter string, will exclude events with InitiatorIP 192.168.25.3 and events with ResponderIP 10.10.10.1

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

Use the OR NOT operator to include search results that exclude certain elements. The OR NOT operator cannot be used at the beginning of a search string.

For example, this search string will find events with the Protocol of TCP, OR that have the InitiatorIP of 10.10.10.43, or those NOT from InitiatorPort 59614.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

You could also think of it this way: Search for (Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614").

Wildcard Searches

Use an asterisk (*) to represent a wildcard in the value field of an **attribute:value** search to find results within events. For example, this filter string,

```
URL:*feedback*
```

will find strings in the URL attribute field of events that contain the string **feedback**.

Related Information:

- Show and Hide Columns on the Event Logging Page
- Event Attributes in Security Analytics and Logging

Search Historical Events in the Background

Security Cloud Control provides you the ability to define a search criteria and search for event logs based on any defined search criteria. Using the background search capability, you can also perform event log searches in the background, and view the search results once the background search is completed.

Based on the subscription alert and service integrations you have configured, you are notified once the background search has been completed.

You can view, download, or delete the search results directly from the **Background Searches** page. You can also schedule a background search to occur for a one-time event or schedule a recurring schedule. Navigate to the **Notification Settings** page to view or modify the subscription options.

Search for Events in the Events Logging Page

Use the search and background search capabilities to view all logged events in the **Event Logging** page. Note that background searches can only be performed for historical events.

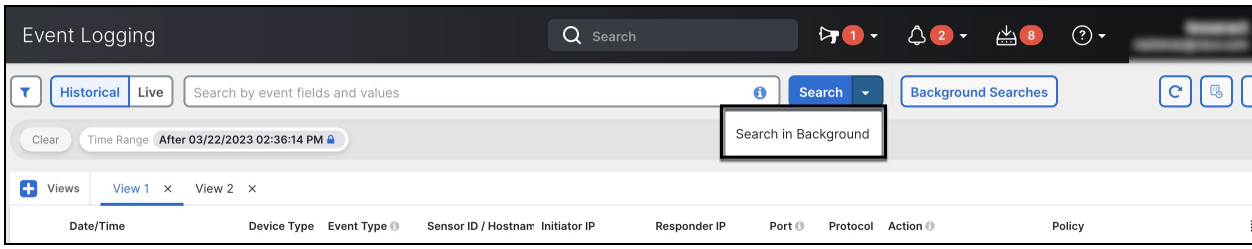
Procedure

Step 1 In the navigation bar, choose **Events & Logs** > **Events**.

Step 2 Click either the **Historical** or **Live** tab.

Step 3 Navigate to the search bar, type the search expression, and enter the **Search** button to execute the search. You can narrow or expand the search with an Absolute Time Range or Relative Time Range.

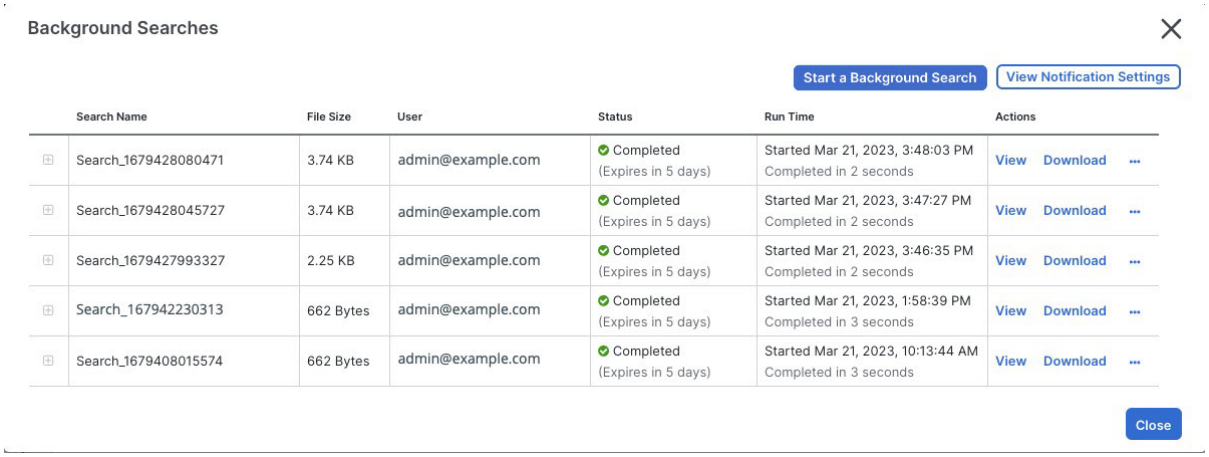
Alternatively, from the **Search** drop-down list, choose **Search in Background** to execute the search in the background while you move away from the search page. You are notified when the search results are ready.



If you click the **Search** button, the results directly appear in the event table. Upon selecting any specific search result, the search criteria appears in the search bar for an easy reference.

If you choose to execute the search in the background, the search operation is queued, and you are notified once the search is completed. You are allowed to execute multiple search queries in the background.

Step 4 Click the **Background Searches** button to view the Background Searches page.



The Background Searches page displays a list of search results. You can choose to view, download, or delete the search results. You can also navigate to the Notification Settings page to view or modify the subscription options. Select the **Start a Background Search** button to initiate a search from this page.

What to do next

You can turn any background search into a scheduled background search if you need a recurring query. See Schedule a Background Search in the Event Viewer, on page 706 for more information.

Schedule a Background Search in the Event Viewer

Schedule a recurring query in the background in the event viewer page. You can modify or cancel the scheduled search at any time. You can also modify an existing query to be a recurring search.

Note

- You can schedule a background search only for historical events.
- You can opt to get alerts on searches that have started, completed, or have failed.

Use the following steps to create a scheduled background search:

Procedure

Step 1 In the navigation bar, choose **Events & Logs** > **Events**.

Step 2 Click the **Historical** tab to view historical events.

Step 3 In the search bar, type the search expression you want to search for. Click the **Search** drop-down button and choose **Search in Background**.

Step 4 (Optional) Rename the search.

Step 5 The **Search now** check box is checked by default. When checked, the search starts upon saving; if unchecked, the background query runs only as a future search.

Step 6 Check the **Setup recurring schedule** and configure the following settings:

- **Search Logs for the Last**: How far back you want to search through.
- **Frequency**: How frequent you want the scheduled search to occur.

Step 7 Confirm the scheduled search criteria at the bottom of the window. Click **Schedule and Search Now**. If you did not opt for the search to start immediately, click **Schedule Search**.

What to do next

Results from a scheduled background search are available for review for up to 7 days before Security Cloud Control automatically deletes them.

Download a Background Search

Search results and schedules queries are stored for seven days before Security Cloud Control automatically removes them. Download a copy of the background search in .CSV format.

Procedure

Step 1 In the left pane go to **Events & Logs** > **Events**.

Step 2 Click **Background Searches** > **Actions** > **Download**.

Step 3 Locate your search. Scheduled searches are stored under the **Queries** tab.

Step 4 Click **Download**. The background search file in .CSV format gets automatically downloaded to the default storage location on your local drive.

Data Storage Plans

You need to purchase a data storage plan that corresponds to the volume of events the Cisco cloud receives from your onboarded ASA and FTD devices on a daily basis. This volume is referred to as your daily ingest rate. Data plans are available in whole number amounts of GB/day and in 1-, 3-, or 5-year terms. The most effective method to determine your ingest rate is to participate in a free trial of Secure Logging Analytics (SaaS) before making a purchase. This trial will provide an accurate estimate of your event volume.

By default, you receive 90 days of rolling data storage. This policy ensures that the most recent 90 days of events are stored in the Cisco cloud, and data older than 90 days is deleted.

You have the option to upgrade to additional event retention beyond the default 90 days or to increase daily volume (GB/day) through a change order to an existing subscription. Billing for these upgrades will be prorated for the remainder of the subscription term.

See the Secure Logging Analytics (SaaS) Ordering Guide for all the details about data plans.

Note If you have a Security Analytics and Logging license and data plan, then obtain a different Security Analytics and Logging license, you are not required change your data plan. Similarly, if your network traffic throughput changes and you obtain a different data plan, this change alone does not require you to obtain a different Security Analytics and Logging license.

What data gets counted against my allotment?

All events sent to the Secure Event Connector accumulate in the Secure Logging Analytics (SaaS) cloud and count against your data allotment.

Filtering what you see in the events viewer does not decrease the number of events stored in the Secure Logging Analytics (SaaS) cloud, it reduces the number of events you can see in the events viewer.

We're using up our storage allotment quickly, what can we do?

Here are two approaches to address that problem:

- Request more storage.
- Consider reducing the number of rules that log events. You can log events from SSL policy rules, security intelligence rules, access control rules, intrusion policies, and file and malware policies. Review what you are currently logging to determine if it is necessary to log events from as many rules and policies.

Extend Event Storage Duration and Increase Event Storage Capacity

Security Analytics and Logging customers receive 90 days of event storage when they purchase any of these Licensing.

- **Logging and Troubleshooting**
- **Logging Analytics and Detection**
- **Total Network Analytics and Monitoring**

You can choose to upgrade your license to have 1, 2, or 3 years worth of rolling event storage at the time you first purchase your license or at any time during the duration of your license.

At the time you first purchase your Security Analytics and Logging license, you will be asked if you want to upgrade your storage capacity. If you answer, "yes," an additional Product Identifier (PID) will be added to the list of PIDs you are purchasing.

To obtain security analytics and logging entitlement, you can purchase one of the following licenses:

- **Cisco Defense Orchestrator Device License Subscription with Unlimited Logging**: This license combines Cisco Defense Orchestrator management license for managing Cisco firewalls device with unlimited volume of event logging. By default, 90 days of storage retention is available with this license. You have the option to extend log retention period to 1, 2, or 3 years by purchasing additional data retention extension licenses.
- **Cisco Logging and Troubleshooting License Subscription**: This license supports logging 1 GB volume per day with 90 days of storage retention. You can extend log retention to 1, 2, or 3 years by purchasing additional data retention extension licenses.

For more information, see About Security Cloud Control Licenses.

To extend your rolling event storage or increase the amount of event cloud storage, do the following steps:

Procedure

Step 1 Log in to your account on Cisco Commerce.

Step 2 Select your Security Cloud Control PID.

Step 3 Follow the prompts to upgrade the length or capacity of your storage capacity.

The increased cost will be pro-rated based for the term remaining on your existing license. See the Guidelines for Quoting Cisco Defense Orchestrator Products for detailed instructions.

View Security Analytics and Logging Data Plan Usage

To see your monthly logging limit, the amount of storage you have used, and when the usage period resets to zero, do the following:

Procedure

Step 1 From the left navigation bar, click **Administration** > **Log Settings**.

Step 2 You can also click **View Historical Usage** to see up to the last 12 months of storage usage.

Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS)

Secure Logging Analytics (SaaS) allows you to send events from your ASA or FDM-managed devices to certain UDP, TCP, or NSEL ports on the Secure Event Connector (SEC). The SEC then forwards those events to the Cisco cloud.

If these ports aren't already in use, the SEC makes them available to receive events and the Secure Logging Analytics (SaaS) documentation recommends using them when you configure the feature.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

If those ports are already in use, before you configure Secure Logging Analytics (SaaS), look at your SEC device details to determine what ports it is actually using to receive events.

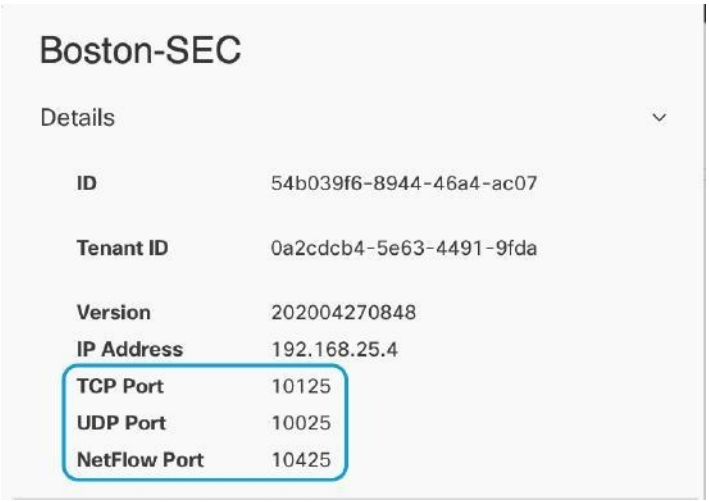
To find the port numbers the SEC uses:

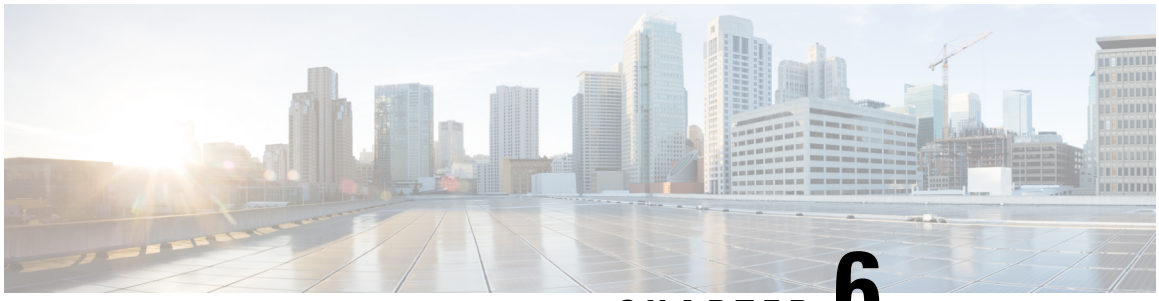
Procedure

Step 1 From the left pane, click **Administration** > **Firewall Management Center** and then click the **Secure Connectors** tab.

Step 2 In the **Secure Connectors** page, select the SEC you want to send events to.

Step 3 In the **Details** pane, you will see the TCP, UDP, and NetFlow (NSEL) port you should send events to.





CHAPTER 6

Integrating Security Cloud Control with Cisco Security Cloud Sign On

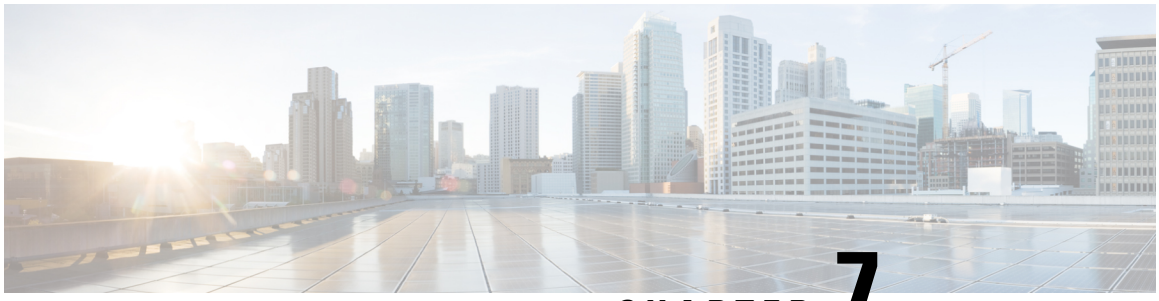
Merge Your Security Cloud Control and Cisco XDR Tenant Accounts

If your Secure Firewall Threat Defense or On-Premises Firewall Management Center is used with Security Cloud Control or Cisco Security Analytics and Logging (SaaS) and Cisco XDR, you must link your Security Cloud Control tenant account with the Cisco XDR tenant account associated with the device.

Be mindful of when you initiate this process. This merging process may take an extended amount of time.

See Merge Accounts for instructions.

Note If you have accounts on more than one regional cloud, you must merge accounts separately for each regional cloud.



CHAPTER 7

Terraform

About Terraform

Security Cloud Control customers can use the Security Cloud Control Terraform provider and Security Cloud Control Terraform modules to rapidly set up their tenants using code that is repeatable and version-controlled. The Security Cloud Control Terraform provider allows users to do the following:

- **Manage** users
- **Onboard** Secure Firewall Threat Defense devices on cloud-delivered Firewall Management Centers, Cisco Secure ASA devices, and iOS devices
- **Onboard** secure device connectors on vSphere and AWS
- **Onboard** secure event connectors on AWS

For more information, refer to the following pages:

- Security Cloud Control Terraform Provider page
- Security Cloud Control SDC on vSphere module page
- Security Cloud Control SDC on AWS module page
- Security Cloud Control SEC on AWS module page
- Work through the Devnet learning lab
- Automating Security Infrastructure Management Using the Cisco Security Cloud Control Terraform Provider - Learning Lab
- Security Cloud Control automation examples on GitHub

Support

The Security Cloud Control Terraform provider and modules are published as Open Source Software under the Apache 2.0 license. Please file issues on GitHub in the repositories below if you require support:

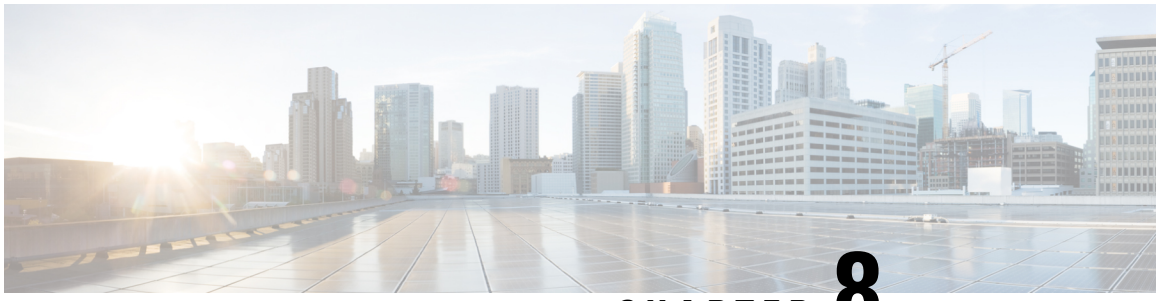
Module	Repository
Security Cloud Control Terraform Provider	https://github.com/ciscodevnet/terraform-provider-SecurityCloud Control
Security Cloud Control SDC Module (vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-SecurityCloud Control-sdc
Security Cloud Control SDC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-SecurityCloud Control-sdc
Security Cloud Control SEC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-SecurityCloud Control-sec

Contribution to Repositories

The Security Cloud Control team welcomes contributions to the repositories above. Please create pull pequests on these GitHub repositories if you wish to contribute to improving the provider and modules.

Related Topics

- Deploy an SDC to vSphere Using Terraform
- Deploy an SDC to AWS VPC Using Terraform
- Deploy an SEC to AWS VPC Using Terraform



CHAPTER 8

Troubleshooting

This chapter covers the following sections:

Troubleshoot FDM-Managed Devices

Use the following article to troubleshoot your FDM-managed devices:

- Troubleshooting Device Registration Failure during Onboarding with a Registration Key
- Troubleshoot FDM-Managed HA Creation, on page 724

Troubleshoot the Executive Summary Report

You may go to generate a Network Operations Report and not see the results you are expecting, or any data at all. In some cases, the summaries may display **No data available**. Consider the following scenarios:

- Security Cloud Control polls for events every **hour** from the time the device is onboarded. Some scheduled events can trigger multiple jobs that are polled at varying time intervals, from every 10 minutes, 60 minutes, 6 hours, or 24 hours. If the selected devices have just been onboarded, there may not be enough time to collect and compile data.
- You may have insufficient smart licenses. Only devices that have sufficient licenses generate data. See FDM-Managed Device Licensing Types, on page 196 to determine which smart licenses you required to generate the desired data.
- Logging is not enabled for access control rules. See Logging Settings in an FDM-Managed Access Control Rule, on page 343 for more information.
- The time range you selected may have an insufficient amount of data to display, or an access control rule may not have been triggered within the selected time range. Toggle between the **Time Range** options and determine if a different time period affects the report.

Troubleshoot FDM-Managed Device Onboarding

Connectivity

- Check device connectivity with a ping. Try to ping FP management IP address from ASA directly. If the ICMP blocks communication from outside, you will not be able to ping FP management interface from the Internet. cUrl / wget helps to check if FP management interface is accessible on configured IP/Port.
- Check ASA and/or ASDM software versions for compatibility. See Devices, Software, and Hardware Supported by Security Cloud Control for more information.
- Use the ASA logs to identify if Security Cloud Control traffic is blocked by the ASA. Through SSH, attempts to connect to FP HTTP management interface are logged in **/var/log/httpd/httpsd_access_log**.

Module Misconfiguration

- Unsupported configuration. Security Cloud Control may not be able to support the device's configuration if the module does not meet specific requirements.

HTTP Authentication

- Security Cloud Control issues an token-based SSO to authenticate an ASA device during the onboarding process. A token issue may be caused by attempt to onboard FP module from non-admin context in case of ASA in multi-context mode. Invalid tokens are identified as **ASDM SSO logins** in **/var/log/mojo/mojo.log a**

Failed Because of Insufficient License

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.
- If the device status doesn't change, refresh the Security Cloud Control portal by signing out from Security Cloud Control and signing back to resolve any network communication glitch between license server and device.
- If the portal refresh doesn't change the device status, perform the following:

Procedure

Step 1 Generate a new new registration key from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.

Step 2 In the left pane, click the **Inventory** page.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab and select the device with the **Insufficient License** state.

Step 5 In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.

Step 6 In the **Activate** field, paste the new registration key and click **Register Device**.

Once the new registration key is applied successfully to the device, its connectivity state turns to **Online**.

Related Information:

- Onboard a Threat Defense Device
- Onboard an FDM-Managed Device Using Username, Password, and IP Address, on page 166
- Applying or Updating a Smart License

Troubleshoot Device Unregistered

The FDM-managed device may have been unregistered from the cloud via Firewall device manager.

Perform the following to register the device again on the cloud:

Procedure

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the **FTD** tab and select the device in the "Device Unregistered" state, and see the error message on the right.

Step 3 If the unregistered device was onboarded using the registration key, Security Cloud Control prompts you to generate a new registration key as the previously applied key has expired.

a) Click the Refresh button to generate a new registration key and then click the Copy icon .
b) Log into the Firewall device manager of the device you want to reregister with Security Cloud Control.
c) Under **System Settings**, click **Cloud Services**.
d) In the Security Cloud Control area, expand **Get Started**.
e) In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.
f) Click **Register** and then **Accept** the Cisco Disclosure. Firewall device manager sends the registration request to Security Cloud Control.
g) Refresh the **Inventory** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
h) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.

Step 4 If the unregistered device was onboarded using the serial number, Security Cloud Control prompts you to auto-enroll the device from Firewall device manager.

a) Log into the Firewall device manager of the device you want to reregister with Security Cloud Control.
b) Under **System Settings**, click **Cloud Services**.
c) Select the **Auto-enroll with Tenancy from Security Cloud Control** option and click **Register**.
d) Refresh the **Inventory** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
e) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.

Troubleshooting Device Registration Failure during Onboarding with a Registration Key

Failed to Resolve Cloud Service FQDN

If the device registration fails due to failure in resolving cloud service FQDN, check network connectivity or the DNS configuration and attempt to onboard the device again.

Failed Because of an Invalid Registration Key

If the device registration fails due to an invalid registration key, which may occur when you paste incorrect registration key in Firewall device manager.

Copy the same registration key from Security Cloud Control again and attempt to register the device. If the device is already smart licensed, ensure that you remove the smart license before pasting the registration key in firewall device manager.

Failed Because of Insufficient License

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.
- If the device status doesn't change, refresh the Security Cloud Control portal by signing out from Security Cloud Control and signing back to resolve any network communication problems between license server and device.
- If the portal refresh doesn't change the device status, perform the following:
  1. Generate a new new registration key from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.
  2. In the Security Cloud Control navigation bar, click the **Inventory** page.
  3. Select the device with the **Insufficient License** state.
  4. In the **Device Details** pane, click **Manage Licenses** appearing in Insufficient Licenses. The Manage Lincenses window opens.
  5. In the **Activate** field, paste the new registration key and click **Register Device**.
- Once the new registration key is applied successfully to the device, its connectivity state turns to **Online**.

Troubleshoot Intrusion Prevention System

What are my IPS policy options?

Every onboarded device is automatically associated a Security Cloud Control-provided IPS policy called "Default Overrides". Security Cloud Control generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. If you want to use the default IPs policy but modify the signature overrides options, see Firepower Intrusion Policy Signature Overrides for more information. Note that

configuring different signature overrides per device may cause the default overrides policy to become inconsistent.

How do I have a different IPS policy for every device?

Security Cloud Control generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. You do not have to rename the Security Cloud Control-provided IPS policy after each device is onboarded. Expanding the policy displays the devices that are associated with it, and you can also filter the threat events page and the signature overrides page per device or policy. To customize the default overrides policy, configure signature overrides per device. This will cause the default overrides intrusions policy to become inconsistent, but this does not inhibit any functionality.

I onboarded a device that has an override configured from an FDM-managed device.

Overrides that are configured outside of Security Cloud Control do not pose an issue to device configuration or functionality.

If you onboard a device that has an override already configured and this new device shares an IPs policy with a device that does **not** have an override, the IPS policy will be displayed as **inconsistent**. See Step 3 in Firepower Intrusion Policy Signature Overrides to address inconsistencies.

Troubleshooting SSL Decryption Issues

Handling Web Sites Where Decrypt Re-sign Works for a Browser but not an App (SSL or Certificate Authority Pinning)

Some apps for smart phones and other devices use a technique called SSL (or Certificate Authority) pinning. The SSL pinning technique embeds the hash of the original server certificate inside the app itself. As a result, when the app receives the resigned certificate from the FDM-managed device, the hash validation fails and the connection is aborted.

The primary symptom is that users cannot connect to the web site using the site's app, but they can connect using the web browser, even when using the browser on the same device where the app fails. For example, users cannot use the Facebook iOS or Android app, but they can point Safari or Chrome at https://www.facebook.com/ and make a successful connection.

Because SSL pinning is specifically used to avoid man-in-the-middle attacks, there is no workaround. You must choose between the following options:

- Support app users, in which case you cannot decrypt any traffic to the site. Create a Do Not Decrypt rule for the site's application (on the Application tab for the SSL Decryption rule) and ensure that the rule comes before any Decrypt Re-sign rule that would apply to the connections.
- Force users to use browsers only. If you must decrypt traffic to the site, you will need to inform users that they cannot use the site's app when connecting through your network, that they must use their browsers only.

More Details

If a site works in a browser but not in an app on the same device, you are almost certainly looking at an instance of SSL pinning. However, if you want to delve deeper, you can use connection events to identify SSL pinning in addition to the browser test.

There are two ways an app might deal with hash validation failures:

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the server. The Alert is usually an "Unknown CA (48)" alert indicating SSL Pinning. A TCP Reset is sent following the Alert message. You should see the following symptoms in the event details:
  - SSL Flow Flags include ALERT_SEEN.
  - SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.
  - SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.
- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is done and then send a TCP Reset. You should see the following symptoms in the event:
  - SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.
  - SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.

Download Button for CA Certificate is Disabled

The download button is disabled for certificates (self signed and uploaded) that are staged on Security Cloud Control but have not been deployed back to the device yet. A certificate can be downloaded only after deploying it to the device.

Troubleshoot FDM-Managed Device Onboarding Using Serial Number

- Provisioning Error
  - Device Password Has Not Been Changed
  - Device Password Has Already Been Changed
- Claim Error
  - Invalid Serial Number
  - Device Serial Number Already Claimed
  - Device is Offline
  - Failed to Claim the Device

Claim Error

Invalid Serial Number

An incorrect serial number has been entered while claiming the device in Security Cloud Control.

Resolution

1. Delete the FDM-managed device instance in Security Cloud Control.
2. Create a new FDM-managed device instance by entering the correct serial number and claim the device.

Device Serial Number Already Claimed

The following error occurs when you are onboarding the FDM-managed device using its serial number.

Cause

This error can occur for one of the following reasons:

- The device may have been purchased from an external vendor, and the device is in the vendor's tenancy.
- The device may have been previously managed by another Security Cloud Control instance in a different region and is registered to its cloud tenancy.

Resolution

You need to unregister the device's serial number from other cloud tenancy and then reclaim it in your tenant.

Prerequisite

The device must be connected to the Internet that can reach the cloud tenancy.

Device Purchased from an External Vendor

The device purchased from an external vendor may have been registered to the vendor's cloud tenancy.

1. Delete the device instance from Security Cloud Control.
2. Install the FXOS image on the device. For more information, see the "Reimage Procedures" chapter of the Cisco FXOS Troubleshooting Guide for the Firepower 1000/21000 with FTD guide.
3. Connect to the FXOS CLI from the console port.
4. Log in to FXOS using your current admin password.
5. In the FXOS CLI, connect to local-mgmt: firepower # **connect local-mgmt**.
6. Execute the command to deregister the device from the cloud tenancy. firepower(local-mgmt) # **cloud deregister**.
7. On successful deregistration, the CLI interface returns a success message.

   Example: **firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9**

   If the device was already unregistered from the cloud tenancy, the CLI interface indicates that the device serial number was not registered with cloud tenancy. **RESULT=success MESSAGE=DEVICE_NOT_FOUND: Device with serial number JAD213082x9 is not registered with** Security Services Exchange **, X-Flow-Id: 63e48b4c-8426-48fb-9bd0-25fcd7777b99**

8. Claim the device again in Security Cloud Control by providing its serial number. See Onboard an FDM-Managed Device using the Device's Serial Number for more information.
9. Install the FDM-managed device application (version 6.7 or later) on the device. The zero-touch provisioning is initiated on the device and it registers itself in the Cisco Cloud. Security Cloud Control onboards the device.

Onboard an FDM-Managed Device Already Managed by Another Cloud Tenancy in a Different Region

The device may have been previously managed by another Security Cloud Control instance in a different region and is registered to its cloud tenancy.

Case 1: You have access to the tenant that owns the device.

1. Delete the device instance from the Security Cloud Control in region 1.
2. In Firewall device manager, go to **System Settings** > **Cloud Services** page. A warning message appears indicating that the device has been removed from Security Cloud Control.
3. Click the link and select **Unregister Cloud Services** from the drop-down list.
4. Read the warning and click **Unregister**.
5. Claim the device from Security Cloud Control in region 2.
6. In Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Security Cloud Control** option and click **Register**. The device maps to the new tenant that belongs to the new region and Security Cloud Control onboards the device.

Case 2: You don't have access to the tenant that owns the device.

1. Connect to the FXOS CLI from the console port.
2. Log in to FXOS using your current admin password.
3. In the FXOS CLI, connect to local-mgmt: firepower # **connect local-mgmt**.
4. Execute the command to deregister the device from the cloud tenancy. firepower(local-mgmt) # **cloud deregister**.
5. On successful deregistration, the CLI interface returns a success message.

   Example: **firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9**

   The device is unregistered from the cloud.
6. Claim the device from Security Cloud Control in region 2.
7. In Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Security Cloud Control** option and click **Register**. The device maps to the new tenant that belongs to the new region and Security Cloud Control onboards the device.

Device is Offline

Cause

The device is unable to reach the Cisco Cloud due to one of the following reasons:

- The device is cabled incorrectly.
- Your network may require a static IP address for the device.
- Your network uses custom DNS, or there is external DNS blocking on the customer network.
- PPPoE authentication is needed. (Common in Europe region.)
- The FDM-managed device is behind a proxy.

Resolution

1. Sign in to the device and go through the bootstrap CLI process or the Security Cloud Control Easy setup process to configure the device first so it can reach the Internet.
2. Check the cabling and network connectivity.
3. Ensure that your firewall is not blocking any traffic.
4. Ensure that the Security Services Exchange domains are reachable. See Onboard a Secure Firewall Threat Defense Device With Zero-Touch Provisioning for more information.

Failed to Claim the Device

Cause

This error may occur due to one of the following reasons:

- Security Services Exchange may have temporary issues.
- The server may be down.

Resolution

1. Delete the FDM-managed device instance in Security Cloud Control.
2. Create a new FDM-managed device instance and claim the device again after some time.

Note If you are not able to claim the device, go to the workflows to see the error message and send the details to the Security Cloud Control support team.

Provisioning Error

Device Password Has Not Been Changed

When claiming the device from Security Cloud Control, the device's initial provisioning may fail and display an "Unprovisioned" message in the **Inventory** page.

Cause

You may have selected the "Default Password Changed" option in the Security Cloud Control FDM-managed device serial number onboarding wizard for a new FDM-managed device whose default password was not changed.

Resolution

You need to click **Enter Password** in the **Inventory** page to change the device's password. Security Cloud Control continues with the new password and onboards the device.

Device Password Has Already Been Changed

When claiming the device from Security Cloud Control, the device's initial provisioning may fail and display an "Unprovisioned" message in the **Inventory** page.

Cause

You may have selected the "Default Password Not Changed" option in the Security Cloud Control FDM-managed device serial number onboarding wizard for an FDM-managed device whose default password has already been changed.

Resolution

You need to click **Confirm and Proceed** in the **Inventory** page to ignore the new password provided in the serial onboarding wizard. Security Cloud Control continues with the old password and onboards the device.

For Other Errors

For all other provisioning errors, you can click **Retry** to reinitiate the provisioning. If it fails even after multiple retries, perform the following steps:

1. Delete the FDM-managed device instance from Security Cloud Control and create a new instance. See Onboard an FDM-Managed Device using the Device's Serial Number for onboarding steps.
2. In Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Security Cloud Control** option and click**Register**.

Troubleshoot FDM-Managed HA Creation

Event Description Error

If you attempt to onboard or create an FDM-managed HA pair in Security Cloud Control, the HA pair may fail to form and you may see an error with the following message:

```
Event description: CD App Sync error is Cisco Threat Response is enabled on Active but not on Standby
```

If you see this error, then one or both of the devices within the HA pair is not configured to allow the devices to send events to the a Cisco cloud server such as Security Cloud Control, Firepower Threat Response, Or the Cisco Success Network.

You **must** enable the **Send Events to the Cisco Cloud** feature from the Firewall device manager UI. See the **Configuring Cloud Services** chapter of the Firepower Device Manager Configuration Guide of the version you are running for more information.

One of my devices is in a bad state after creating HA

If one of the devices falls into an unhealthy or **failed** state during HA creation, break the HA pair and resolve the device's state, then recreate HA. The FDM-Managed High Availability Failover History might help diagnose the issue.

Troubleshoot a Secure Device Connector

Use these topics to troubleshoot an on-premises Secure Device Connector (SDC).

If none of these scenarios match yours, How Security Cloud Control Customers Open a Support Ticket with TAC.

SDC is Unreachable

An SDC is in the state "Unreachable" if it has failed to respond to two heartbeat requests from Security Cloud Control in a row. If your SDC is unreachable, your tenant will not be able to communicate with any of the devices you have onboarded.

Security Cloud Control indicates that an SDC is unreachable in these ways:

- You see the message, “Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs.” on the Security Cloud Control home page.
- The SDC's status in the Services page is "Unreachable."

Frist, attempt to reconnect the SDC to your tenant to resolve this issue:

1. Check that the SDC virtual machine is running and can reach a Security Cloud Control IP address in your region. See Connect Security Cloud Control to your Managed Devices, on page 15.
2. Attempt to reconnect Security Cloud Control and the SDC by requesting a heartbeat manually. If the SDC responds to a heartbeat request, it will return to "Active" status. To request a heartbeat manually:
   a. In the left pane, choose **Tools & Services** > **Secure Connectors**.
   b. Click the SDC that is unreachable.
   c. In the Actions pane, click **Request Heartbeat**.
   d. Click **Reconnect**.
3. If the SDC does not return to the Active status after manually attempting to reconnect it to your tenant, follow the instructions in SDC Status not Active on Security Cloud Control after Deployment, on page 725.

.

SDC Status not Active on Security Cloud Control after Deployment

If Security Cloud Control does not indicate that your SDC is active in about 10 minutes after deployment, connect to the SDC VM using SSH using the `Security Cloud Control` user and password you created when you deployed the SDC.

Procedure

Step 1 Review `/opt/cdo/configure.log`. It shows you the configuration settings you entered for the SDC and if they were applied successfully. If there were any failures in the setup process or if the values weren't entered correctly, run the sdc-onboard setup again:

a) At the prompt enter`sudo sdc-onboard setup`.
b) Enter the password for the `cdo` user.
c) Follow the prompts. The setup script guides you through all the configuration steps you took in the setup wizard and gives you an opportunity to make changes to the values you entered.

Step 2 If after reviewing the log and running `sudo sdc-onboard setup`, Security Cloud Control still does not indicate that the SDC is **Active**, Contact Security Cloud Control Support.

Changed IP Address of the SDC is not Reflected in Security Cloud Control

If you changed the IP address of the SDC, it will not be reflected in Security Cloud Control until after 3:00 AM GMT.

Troubleshoot Device Connectivity with the SDC

Use this tool to test connectivity from Security Cloud Control, through the Secure Device Connector (SDC) to your device. You may want to test this connectivity if your device fails to onboard or if you want to determine, before on-boarding, if Security Cloud Control can reach your device.

Procedure

Step 1 In the left pane, click **Administration** > **Firewall Management Center**, and click the **Secure Connectors** tab.

Step 2 Select the SDC.

Step 3 In the **Troubleshooting** pane on the right, click **Device Connectivity**.

Step 4 Enter a valid IP address or FQDN and port number of the device you are attempting to troubleshoot, or attempting to connect to, and click **Go**. Security Cloud Control performs the following verifications:

a) **DNS Resolution** - If you provide a FQDN instead of an IP address, this verifies the SDC can resolve the domain name and acquires the IP address.
b) **Connection Test** - Verifies the device is reachable.
c) **TLS Support** - Detects the TLS versions and ciphers that both the device and the SDC support.

- **Unsupported Cipher** - If there are no TLS version that are supported by both the device and the SDC, Security Cloud Control also tests for TLS versions and ciphers that are supported by the device, but not the SDC.

d) SSL Certificate - The troubleshoot provides certificate information.

Step 5 If you continue to have issues onboarding or connecting to the device, Contact Security Cloud Control Support.

Intermittent or No Connectivity with SDC

The solution discussed in this section applies only to an on-premise Secure Device Connector (SDC).

Symptom: Intermittent or no connectivity with SDC.

Diagnosis: This problem may occur if the disk space is almost full (above 80%).

Perform the following steps to check the disk space usage.

1. Open the console for your Secure Device Connector (SDC) VM.
2. Log in with the username **cdo**.
3. Enter the password created during the initial login.
4. First, check the amount of free disk space by typing **`df -h`** to confirm that there is no free disk space available.

   You can confirm that the disk space was consumed by the Docker. The normal disk usage is expected to be under 2 Gigabytes.
5. To see the disk usage of the **Docker** folder,

   execute **`sudo du -h /var/lib/docker | sort -h`**.

   You can see the disk space usage of the **Docker** folder.

Procedure

If the disk space usage of the Docker folder is almost full, define the following in the docker config file:

- Max-size: To force a log rotation once the current file reaches the maximum size.
- Max-file: To delete excess rotated log files when the maximum limit it reached.

Perform the following:

1. Execute **`sudo vi /etc/docker/daemon.json`**.
2. Insert the following lines to the file.

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. Press **ESC** and then type **`:wq!`** to write the changes and close the file.

Note You can execute **`sudo cat /etc/docker/daemon.json`** to verify the changes made to the file.

4. Execute **sudo systemctl restart docker** to restart the docker file.

   It will take a few minutes for the changes to take effect. You can execute **sudo du -h /var/lib/docker | sort -h** to see the updated disk usage of the docker folder.

5. Execute **df -h** to verify that the free disk size has increased.

6. Before your SDC status can change from Unreachable to Active, you must go to the **Secure Connectors** tab which you can navigate to from **Administration** > **Firewall Management Center** and click **Request Reconnect** from the Actions menu.

Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc

The Cisco Product Security Incident Response Team (PSIRT) published the security advisory **cisco-sa-20190215-runc** which describes a high-severity vulnerability in Docker. Read the entire PSIRT team advisory for a full explanation of the vulnerability.

This vulnerability impacts all Security Cloud Control customers:

- Customers using Security Cloud Control's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the Security Cloud Control Operations Team.
- Customers using an SDC deployed on-premise need to upgrade their SDC host to use the latest Docker version. They can do so by using the following instructions:
  - Updating a Security Cloud Control-Standard SDC Host, on page 728
  - Updating a Custom SDC Host, on page 729
  - Bug Tracking, on page 729

Updating a Security Cloud Control-Standard SDC Host

Use these instructions if you Deploy a Secure Device Connector Using Security Cloud Control's VM Image

Procedure

Step 1 Connect to your SDC host using SSH or the hypervisor console.

Step 2 Check the version of your Docker service by running this command:

```
docker version
```

Step 3 If you are running one of the latest virtual machines (VMs) you should see output like this:

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
```

```
 OS/Arch: linux/amd64
 Experimental: false
```

It's possible you may see an older version here.

Step 4 Run the following commands to update Docker and restart the service:

```
> sudo yum update docker-ce
> sudo service docker restart
```

Note There will be a brief connectivity outage between Security Cloud Control and your devices while the docker service restarts.

Step 5 Run the docker version command again. You should see this output:

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

Step 6 You are done. You have now upgraded to the latest, and patched, version of Docker.

Updating a Custom SDC Host

If you have created your own SDC host you will need to follow the instructions to update based on how you installed Docker. If you used CentOS, yum and Docker-ce (the community edition) the preceding procedure will work.

If you have installed Docker-ee (the enterprise edtion) or used an alternate method to install Docker, the fixed versions of Docker may be different. You can check the Docker page to determine the correct versions to install: Docker Security Update and Container Security Best Practices.

Bug Tracking

Cisco is continuing to evaluate this vulnerability and will update the advisory as additional information becomes available. After the advisory is marked Final, you can refer to the associated Cisco bug for further details:

CSCvo33929-CVE-2019-5736: runc container breakout

Invalid System Time

Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

Note If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because your SDC system time was 15 minutes ahead or behind the AWS system time.

Please follow the steps below to correct the system time issue. Once this problem is resolved, we will be able to proceed with the migration.

Procedure

Step 1 Login to your SDC VM throught the VM terminal or by making an SSH connection.

Step 2 At the prompt, enter `sudo sdc-onboard setup` and authenticate.

Step 3 You are now going to respond to the SDC setup questions as if you are were setting up the SDC for the first time. Re-enter all the same passwords and network information as you had before, except take special note of the NTP server address:

a) Reset the root and Security Cloud Control user passwords with the same passowrds you used to setup the SDC.
b) When prompted, enter **y** to re-configure the network.
c) Enter the value for IP address/CIDR as you had before.
d) Enter the value for the network gateway as you had before.
e) Enter the value for the DNS Server as you had before.
f) When prompted for the NTP server, be sure to provide a valid NTP server address, such as `time.aws.com`.
g) Review the values you provided and enter **y** if they are correct.

Step 4 Validate that your time server is reachable and synchronized with your SDC by entering `date` at the prompt. The UTC date and time are displayed and you can compare it to your SDC time.

What to do next

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can complete your SDC migration to the new communication method.

SDC version is lower than 202311****

Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

Note If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because your tenant is running a version lower than 202311****.

The current version of your SDC is listed on the Secure Connectors page by navigating from the Security Cloud Control menu bar, **Tools & Services** > **Secure Connectors**. After selecting your SDC, its version number is found in the **Details** pane on the right of the screen.

Please follow the steps below to upgrade the SDC version. Once this problem is resolved, Security Cloud Control operations will be able to run the migration process again.

Procedure

Step 1 Log in to the SDC VM and authenticate.

Step 2 At the prompt, enter `sudo su - sdc` and authenticate.

Step 3 At the prompt, enter `crontab -r`.

If you receive the message `no crontab for sdc` you can ignore it and move to the next step.

Step 4 At the prompt, enter `./toolkit/toolkit.sh upgrade`. Security Cloud Control will determine if you need an upgrade and upgrade the toolkit. Ensure that no errors were reported in the console.

Step 5 Verify the new version of the SDC:

a) Log in to Security Cloud Control.

b) Navigate to the Secure Connectors page by navigating from the Security Cloud Control menu bar, **Tools & Services** > **Secure Connectors**.

c) Select your SDC and click **Request Heartbeat** in the **Actions** pane.

d) Validate that the SDC version is 202311**** or later.

What to do next

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can run the migration process again.

Certificate or Connection errors with AWS servers

Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

Note If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because they experienced a connection issue.

Please follow the steps below to correct the connection issue. Once this problem is resolved, we will be able to proceed with the migration.

Procedure

Step 1 Create firewall rules that allow outbound proxy connections, on port 443, to the domains in your region:

- Production tenants in the Australia region:
  - cognito-identity.ap-southeast-2.amazonaws.com
  - cognito-idp.ap-southeast-2.amazonaws.com
  - sns.ap-southeast-2.amazonaws.com
  - sqs.ap-southeast-2.amazonaws.com
- Production tenants in the India region:
  - cognito-identity.ap-south-1.amazonaws.com
  - cognito-idp.ap-south-1.amazonaws.com
  - sns.ap-south-1.amazonaws.com
  - sqs.ap-south-1.amazonaws.com
- Production tenants in the US region:
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- Production tenants in the EU region:
  - cognito-identity.eu-central-1.amazonaws.com
  - cognito-idp.eu-central-1.amazonaws.com
  - sns.eu-central-1.amazonaws.com
  - sqs.eu-central-1.amazonaws.com
- Production tenants in the APJ region:
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

Step 2 You can determine the full list of IP addresses you need to add to your firewall's "allow list" by using one of the commands below.

Note The commands below are for users that have **jq** installed. The IP addresses will be displayed in a single list.

- Production tenants in the US region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- Production tenants in the EU region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- Production tenants in the APJ region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

Note If you don't have **jq** installed, you can use this shortened version of the command:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

What to do next

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can complete your SDC migration to the new communication method.

Secure Event Connector Troubleshooting

If none of these scenarios match yours, How Security Cloud Control Customers Open a Support Ticket with TAC.

Troubleshooting SEC Onboarding Failures

These troubleshooting topics describes many different symptoms related to Secure Event Connector (SEC) onboarding failure.

SEC on-boarding failed

Symptom: SEC on-boarding failed.

Repair: Remove the SEC and onboard it again.

If you receive this error:

1. Remove the Secure Event Connector and its files from the virtual machine container.
2. Update your Secure Device Connector, on page 34. Ordinarily, the SDC is updated automatically and you should not have to use this procedure but this procedure is useful in cases of troubleshooting.
3. Install a Secure Event Connector on an SDC Virtual Machine, on page 627.

Tip Always use the copy link to copy the bootstrap data when on-boarding an SEC.

Note If this procedure does not correct the problem, Event Logging Troubleshooting Log Files and contact your Managed Service Provider or the Cisco Technical Assistance Center.

SEC Bootstrap data not provided

Message: ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

Diagnosis: Boostrap data was not entered into the setup script when prompted.

Repair: Provide the SEC bootstrap data generated in Security Cloud Control UI when prompted for the bootstrap data input when onboarding.

Bootstrap config file does not exist

Message: ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/Security Cloud Control/es_bootstrapdata") does not exist, exiting.

Diagnosis: SEC Bootstrap data file("/usr/local/Security Cloud Control/es_bootstrapdata") is not present.

Repair: Place the SEC bootstrap data generated in Security Cloud Control UI onto the file **/usr/local/**Security Cloud Control**/es_bootstrapdata** and try onboarding again.

1. Repeat onboarding procedure.
2. Copy the bootstrap date.
3. Log into the SEC VM as the 'sdc' user.
4. Place the SEC bootstrap data generated in Security Cloud Control UI onto the file **/usr/local/**Security Cloud Control**/es_bootstrapdata** and try onboarding again.

Decoding bootstrap data failed

Message: ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC boostrap data, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

Diagnosis: Decoding bootstrap data failed

Repair: Regenerate SEC bootstrap data and try onboarding again.

Bootstrap data does not have required information to onboard SEC

Messages:

- ERROR cannot bootstrap Secure Event Connector container for tenant, the Security Services Exchange FQDN not set, exiting.

- ERROR cannot bootstrap Secure Event Connector container for tenant, the Security Services Exchange OTP not set, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: Security
Services
                                        Exchange FQDN not set, exiting.

[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: Security
Services
                                        Exchange FQDN not set, exiting.
```

Diagnosis: Bootstrap data does not have required information to onboard SEC

Repair: Regenerate bootstrapdata and try onboarding again.

Toolkit cron currently running

Message: ERROR SEC toolkit already running, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

Diagnosis: Toolkit cron currently running.

Repair: Retry onboarding command again.

Adequate CPU and memory not available

Message: ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

Diagnosis: Adequate CPU and memory not available.

Repair: Ensure minimum of 4 CPUs and 8 GB RAM are provisioned exclusively for SEC on your VM and try onboarding again.

SEC already running

Message: ERROR Secure Event Connector already running, execute 'cleanup' before onboarding a new Secure Event Connector, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

Diagnosis: SEC already running.

Repair: Run SEC Cleanup Command before onboarding a new SEC.

SEC domain unreachable

Messages:

- Failed connect to api-sse.cisco.com:443; Connection refused
- ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

Diagnosis: SEC domain unreachable

Repair: Ensure the on-premise SDC has Internet connectivity and try onboarding again.

Onboarding SEC command succeeded without errors, but SEC docker container is not up

Symptom: Onboarding SEC command succeeded without errors, but SEC docker container is not up

Diagnosis: Onboarding SEC command succeeded without errors, but SEC docker container is not up

Repair:

1. Log in to the SEC as the 'sdc' user.
2. Check for any errors in SEC docker container startup logs(/usr/local/Security Cloud Control/data/<tenantDir>/event_streamer/logs/startup.log).
3. If so, run SEC Cleanup Command and try onboarding again.

Contact Security Cloud Control Support

If none of these scenarios match yours, How Security Cloud Control Customers Open a Support Ticket with TAC.

Troubleshooting Secure Event Connector Registration Failure

Symptom: Registration of Cisco Secure Event Connector to cloud eventing service fails.

Diagnosis: These are the most common reasons that the SEC fails to register to the eventing cloud service.

- **The SEC is unable to reach the Eventing cloud service from SEC**

  Repair: Ensure that Internet is accessible on port 443 and DNS is configured correctly.

- **Registration failure due to invalid or expired one-time-password in SEC bootstrapdata**

  Repair:

Procedure

Step 1 Log on to the SDC as the 'sdc' user.

Step 2 View the connector log: (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) to check registration state.

If registration has failed due to invalid token, you'll see the error message in the log file something similar to the one below.

context:(*contextImpl).handleFailed] registration - CE2001: Registration failed - Failed to register the device because of invalid token. Retry with a new valid token. - Failed"

Step 3 Run the SEC Cleanup Command step on SDC VM to remove the SEC from Secure Connectors page.

Step 4 Generate new SEC bootstrap data and retry the SEC on-boarding steps.

Troubleshooting Network Problems Using Security and Analytics Logging Events

Here is a basic framework you can use to troubleshoot network problems using the Events Viewer.

This scenario assumes that your network operations team has had a report that a user can't access a resource on the network. Based on the user reporting the issue and their location, the network operations team has a reasonable idea of which firewall controls their access to resources.

Note This scenario also assumes that an FDM-managed device is the firewall managing the network traffic. Security Analytics and Logging does not collect logging information from other device types.

Procedure

Step 1 In the left pane, click **Events & Logs** > **Events**.

Step 2 Click the **Historical** tab.

Step 3 Start filtering events by **Time Range**. By default, the Historical tab shows the last hour of events. If that is the correct time range, enter the current date and time as the **End** time. If that is not the correct time range, enter a start and end time encompassing the time of the reported issue.

Step 4 Enter the IP address of the firewall that you suspect is controlling the user's access in the **Sensor ID** field. If it could be more than one firewall, filter events using **attribute:value** pairs in the search bar. Make two entries and combine them with an OR statement. For example: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

Step 5 Enter the user's IP address in the **Source IP** field in the Events filter bar.

Step 6 If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.

Step 7 Expand the events in the results and look at their details. Here are some details to look at:

- **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.
- **FirewallPolicy** - The policy in which the rule that triggered the event resides.
- **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.
- **UserName** - The user associated with the initiator IP address. The Initiator IP address is the same as the Source IP address.

Step 8 If the rule action is preventing access, look at the FirewallRule and FirewallPolicy fields to identify the rule in the policy that is blocking access.

Troubleshooting NSEL Data Flows

Once you have , use these procedures to verify that NSEL events are being sent from your ASA to the Cisco Cloud and that the Cisco Cloud is receiving them.

Note that once your ASA is configured to send NSEL events to the Secure Event Connector (SEC) and then on to the Cisco Cloud, data does not flow immediately. It could take a few minutes for the first NSEL packets to arrive assuming there is NSEL-related traffic being generated on the ASA.

Note This workflow shows you a straight-forward use of the "flow-export counters" command and "capture" commands to Troubleshoot NSEL Data Flows. See "Packet Captures" CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide and "Monitoring NSEL" in the Cisco ASA NetFlow Implementation Guide for a more detailed discussion of the usage of these commands.

Perform these tasks:

- Verify that NetFlow Packets are Being Sent to the SEC
- Verify that NetFlow Packets are Being Received by the Cisco Cloud

Event Logging Troubleshooting Log Files

The Secure Event Connector (SEC) troubleshoot.sh gathers all event streamer logs and compresses them in a single .tar.gz file.

Use these procedures to create the comparessed .tar.gz file and uncompress the file:

1. Run the Troubleshooting Script, on page 738.
2. Uncompress the sec_troubleshoot.tar.gz file, on page 739.

Run the Troubleshooting Script

The Secure Event Connector (SEC) troubleshoot.sh gathers all event streamer logs and compresses them in a single .tar.gz file. Follow this procedure to run the troubleshoot.sh script:

Procedure

Step 1 Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).

Step 2 Login and then switch to the **root** user:

```
[cdo@localhost ~]$sudo su root
```

Note You could also switch to the sdc user but acting as root you will also receive IP tables information. The IP table information shows that the firewall is running on the device and all the firewall routes. If the firewall is blocking Secure Event Connector TCP or UDP ports, events will not show up in the Event Logging table. The IP Tables will help you determine if that is the case.

Step 3 At the prompt, run the troubleshoot script and specify the tenant name. This is the command syntax:

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

Here is an example:

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

In the command output, you'll see that the sec_troubleshoot file is stored in the **/tmp/troubleshoot** directory on your SDC. The file name follows the convention **sec_troubleshoot-*timestamp*.tar.gz.**

Step 4 To retrieve the file, log in as the Security Cloud Control user and download it using SCP or SFTP.

Here is an example:

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

What to do next

Continue to Uncompress the sec_troubleshoot.tar.gz file, on page 739.

Uncompress the sec_troubleshoot.tar.gz file

The Secure Event Connector (SEC) Run the Troubleshooting Script script gathers all event streamer logs and compresses them in a single sec_troubleshoot.tar.gz file. Follow this procedure to uncompress the sec_troubleshoot.tar.gz file.

1. Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).
2. Login and then switch to the **root** user:

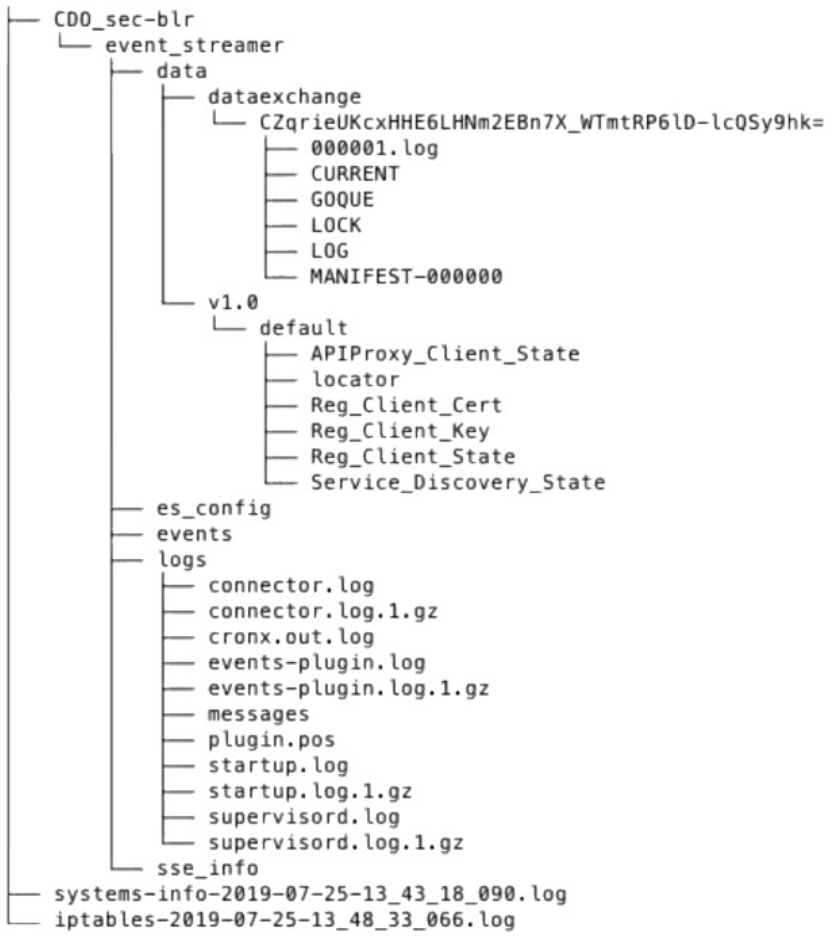
   ```
   [cdo@localhost ~]$sudo su root
   ```

Note You could also switch to the **sdc** user but acting as root you will also receive IP tables information. The IP table information shows that the firewall is running on the device and all the firewall routes. If the firewall is blocking Secure Event Connector TCP or UDP ports, events will not show up in the Event Logging table. The IP Tables will help you determine if that is the case.

3. At the prompt, type the following command:

   ```
   [root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
   ```

The log files are stored in a directory named after your tenant. These are the kinds of logs stored in the sec_troubelshoot-timestamp.tar.gz file. The iptables file is included if you gathered all the log files as the root user.



Generating SEC Bootstrap data failed.

Symptom: While generating SEC bootstrap data in Security Cloud Control, the "bootstrap generation" step fails with the error, "There was an error fetching the bootstrap data. Please try again."

Repair: Retry bootstrap data generation again. If it still fails, How Security Cloud Control Customers Open a Support Ticket with TAC.

SEC Status is Inactive in Security Cloud Control

Symptom: The Secure Event Connector status shows "Inactive" in the Security Cloud Control Secure Connectors page after onboarding for one of these reasons:

- Heartbeat failed
- Connector registration failed

Repair:

- **Heartbeat failed:** Request SEC heartbeat and refresh Secure Connector page to see if the status changes to "Active", if not check if the Secure Device Connector registration failed.

- **Connector registration failed:** Refer issue Troubleshooting Secure Event Connector Registration Failure.

The SEC is "online", but there are no events in Security Cloud Control Event Logging Page

Symptom: The Secure Event Connector shows "Active" in Security Cloud Control Secure Connectors page but you do not see events in Security Cloud Control Event viewer.

Solution or workaround:

Procedure

Step 1 Login to the VM of the on-premise SDC and as the 'sdc' user. At the prompt, type **sudo su - sdc**.

Step 2 Perform these checks:

- Check SEC connector log (/usr/local/Security Cloud Control/data/<tenantDir>/event_streamer/logs/connector.log) and ensure the SEC registration was successful. If not, refer issue "Troubleshooting Secure Event Connector Registration Failure".
- Check SEC events log(/usr/local/Security Cloud Control/data/<tenantDir>/event_streamer/logs/events-plugin.log) and ensure that the events are being processed. If not, How Security Cloud Control Customers Open a Support Ticket with TAC.
- Log in to SEC docker container and execute the command "supervisorctl -c /opt/cssp/data/conf/supervisord.conf " and ensure the output is as shown below and all processes in RUNNING state. IIf not, How Security Cloud Control Customers Open a Support Ticket with TAC.

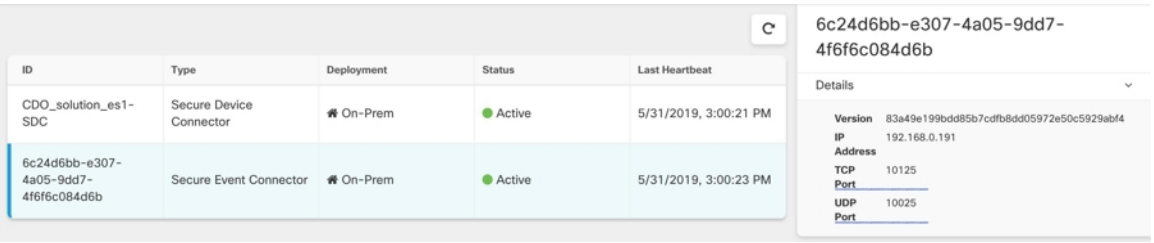
estreamer-connector RUNNING pid 36, uptime 5:25:17

estreamer-cron RUNNING pid 39, uptime 5:25:17

estreamer-plugin RUNNING pid 37, uptime 5:25:17

estreamer-rsyslog RUNNING pid 38, uptime 5:25:17

- Ensure that the firewall rules on the on-premise SDC are not blocking the UDP and TCP ports shown for the SEC on the Secure Connectors page. See Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS) to determine what ports you need to open.



- If you have setup SDC manually using a CentOS 7 VM of your own and have the firewall configured to block incoming requests, you could execute the following commands to unblock the UDP and TCP ports:

firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent

firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent

firewall-cmd --reload

- Using Linux network tools of your choice, check if packets are being received on these ports. If not receiving, re-check the FTD logging configuration.

If none of the above repairs work, How Security Cloud Control Customers Open a Support Ticket with TAC.

SEC Cleanup Command

The Secure Event Connector (SEC) cleanup command removes the SEC container and it's associated files from the Secure Device Connector (SDC) VM. You might run this command in case of a Troubleshooting Secure Event Connector Registration Failure, on page 736 or onboarding failure.

To run the command:

Before you begin

To perform this task you will need to know the name of your tenant. To locate your tenant name, open the user menu in Security Cloud Control and click **Settings**. Scroll down the page to locate your **Tenant Name**.

Procedure

Step 1 Log into the SDC as the `sdc` user. At the prompt, type `sudo su - sdc`.

Step 2 Connect to the `/usr/local/cdo/toolkit directory`.

Step 3 Run `sec.sh remove`*`tenant_name`* and confirm your intent to remove the SEC.

Example:

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

What to do next

If this command failes to remove the SEC, proceed to SEC Cleanup Command Failure, on page 742

SEC Cleanup Command Failure

Use this procedure if the SEC Cleanup Command, on page 742 failed.

Message: SEC not found, exiting.

Symptom: Cleanup SEC command fails to cleanup existing SEC.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

Repair: Manually cleanup Secure Event Connector when cleanup command fails.

Remove already running SEC docker container:

Procedure

Step 1 Log into the SDC as the `sdc` user. At the prompt, type `sudo su - sdc`.

Step 2 Run **docker ps** command to find the names of the SEC container. The SEC name will be in the format, "es_*name*".

Step 3 Run **docker stop** command to stop the SEC container.

Step 4 Run the **rm** command to remove the SEC container.

For example:

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

Use Health Check to Learn the State of your Secure Event Connector

The Secure Event Connector (SEC) Health Check script provides information on the state of your SEC.

Follow this procedure to run Health Check:

Procedure

Step 1 Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).

Step 2 Login to the SDC as "Security Cloud Control" user.

Step 3 Switch to the "sdc" user:

```
[cdo@tenant]$sudo su sdc
```

Step 4 At the prompt, run the healthcheck.sh script and specify the tenant name:

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

For example:

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

The output of the script provides this kind of information:

```
================================================
Running SEC health check for tenant [redacted]
------------------------------------------------
SEC cloud URL [redacted] is: Reachable
------------------------------------------------
SEC Connector status: Active
------------------------------------------------
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
------------------------------------------------
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
================================================
```

Values of Health Check output:

- **SEC Cloud URL**: Displays the Security Cloud Control cloud URL and whether or not the SEC can reach Security Cloud Control.
- **SEC Connector**: Will show "Running" if the SEC connector has been onboarded correctly and has started.
- **SEC UDP syslog server**: Will show "Running" if the UDP syslog server is ready to send UDP events.
- **SEC TCP syslog server**: Will show "Running" if the TCP syslog server is ready to send TCP events.
- **SEC Connector status**: Will show Active if the SEC is running and onboarded to Security Cloud Control.
- **SEC Send sample event**: If at the end of the health check, all the status checks are "green," the tool sends a sample event. (If any of the processes are "Down," the tool skips sending the test event.) The sample event shows up in the Event Log as a policy named "sec-health-check."

Troubleshoot Security Cloud Control

Troubleshooting Login Failures

Login Fails Because You are Inadvertently Logging in to the Wrong Security Cloud Control Region

Make sure you are logging into the appropriate Security Cloud Control region. After you log into https://sign-on.security.cisco.com, you will be given a choice of what region to access.

See Signing in to Security Cloud Control in Different Regions, on page 9 for information about which region you shoud sign into.

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

Solution If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try "forgot password" cannot recover a viable password, you may have tried to login without creating a new Cisco Security Cloud Sign On account, you need to sign up for a new Cisco Security Cloud Sign On Account by following the instructions in Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication, on page 78.

Login to the Cisco Security Cloud Sign On Dashboard Succeeds but You Can't Launch Security Cloud Control

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control and Cisco Secure Sign-On.

Login Fails Using a Saved Bookmark

Solution You may be attempting to log in using an old bookmark you saved in your browser. The bookmark could be pointing to https://cdo.onelogin.com.

Solution Log in to https://sign-on.security.cisco.com.

- **Solution** If you have not yet created a Cisco Secure Sign-On account, Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication.
- **Solution** If you have created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Security Cloud Control APJ
  - **Solution** Cisco Security Cloud Control Australia
  - **Solution** Cisco Security Cloud Control EU
  - **Solution** Cisco Security Cloud Control India
  - **Solution** Cisco Security Cloud Control US
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Access and Certificates

Resolve New Fingerprint Detected State

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device in the **New Fingerprint Detected** state.

Step 5 Click **Review Fingerprint** in the New Fingerprint Detected pane.

Step 6 When prompted to review and accept the fingerprint:

a. Click **Download Fingerprint** and review it.

b. If you are satisfied with the fingerprint, click **Accept**. If you are not, click **Cancel**.

Step 7 After you resolve the new fingerprint issue, the connectivity state of the device may show **Online** and the Configuration Status may show "Not Synced" or "Conflict Detected." Review Resolve Configuration Conflicts to review and resolve configuration differences between Security Cloud Control and the device.

Troubleshooting Network Problems Using Security and Analytics Logging Events

Here is a basic framework you can use to troubleshoot network problems using the Events Viewer.

This scenario assumes that your network operations team has had a report that a user can't access a resource on the network. Based on the user reporting the issue and their location, the network operations team has a reasonable idea of which firewall controls their access to resources.

Note This scenario also assumes that an FDM-managed device is the firewall managing the network traffic. Security Analytics and Logging does not collect logging information from other device types.

Procedure

Step 1 In the left pane, click **Events & Logs** > **Events**.

Step 2 Click the **Historical** tab.

Step 3 Start filtering events by **Time Range**. By default, the Historical tab shows the last hour of events. If that is the correct time range, enter the current date and time as the **End** time. If that is not the correct time range, enter a start and end time encompassing the time of the reported issue.

Step 4 Enter the IP address of the firewall that you suspect is controlling the user's access in the **Sensor ID** field. If it could be more than one firewall, filter events using **attribute:value** pairs in the search bar. Make two entries and combine them with an OR statement. For example: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

Step 5 Enter the user's IP address in the **Source IP** field in the Events filter bar.

Step 6 If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.

Step 7 Expand the events in the results and look at their details. Here are some details to look at:

- **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.
- **FirewallPolicy** - The policy in which the rule that triggered the event resides.
- **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.
- **UserName** - The user associated with the initiator IP address. The Initiator IP address is the same as the Source IP address.

Step 8 If the rule action is preventing access, look at the FirewallRule and FirewallPolicy fields to identify the rule in the policy that is blocking access.

Troubleshooting SSL Decryption Issues

Handling Web Sites Where Decrypt Re-sign Works for a Browser but not an App (SSL or Certificate Authority Pinning)

Some apps for smart phones and other devices use a technique called SSL (or Certificate Authority) pinning. The SSL pinning technique embeds the hash of the original server certificate inside the app itself. As a result, when the app receives the resigned certificate from the Firepower Threat Defense device, the hash validation fails and the connection is aborted.

The primary symptom is that users cannot connect to the web site using the site's app, but they can connect using the web browser, even when using the browser on the same device where the app fails. For example, users cannot use the Facebook iOS or Android app, but they can point Safari or Chrome at https://www.facebook.com and make a successful connection.

Because SSL pinning is specifically used to avoid man-in-the-middle attacks, there is no workaround. You must choose between the following options:

More Details

If a site works in a browser but not in an app on the same device, you are almost certainly looking at an instance of SSL pinning. However, if you want to delve deeper, you can use connection events to identify SSL pinning in addition to the browser test.

There are two ways an app might deal with hash validation failures:

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the server. The Alert is usually an "Unknown CA (48)" alert indicating SSL Pinning. A TCP Reset is sent following the Alert message. You should see the following symptoms in the event details:
  - `SSL Flow Flags include ALERT_SEEN.`
  - `SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.`
  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.`
- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is done and then send a TCP Reset. You should see the following symptoms in the event:
  - `SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.`
  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.`

Troubleshoot Intrusion Prevention System

What are my IPS policy options?

Every onboarded device is automatically associated a Security Cloud Control-provided IPS policy called "Default Overrides". Security Cloud Control generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. If you want to use the default IPs policy but modify the signature overrides options, see Firepower Intrusion Policy Signature Overrides for more information. Note that configuring different signature overrides per device may cause the default overrides policy to become inconsistent.

How do I have a different IPS policy for every device?

Security Cloud Control generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. You do not have to rename the Security Cloud Control-provided IPS policy after each device is onboarded. Expanding the policy displays the devices that are associated with it, and you can also filter the threat events page and the signature overrides page per device or policy. To customize the default overrides policy, configure signature overrides per device. This will cause the default overrides intrusions policy to become inconsistent, but this does not inhibit any functionality.

I onboarded a device that has an override configured from FDM.

Overrides that are configured outside of Security Cloud Control do not pose an issue to device configuration or functionality.

If you onboard a device that has an override already configured and this new device shares an IPs policy with a device that does **not** have an override, the IPS policy will be displayed as **inconsistent**. See Step 3 in Firepower Intrusion Policy Signature Overrides to address inconsistencies.

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

Solution If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try "forgot password" cannot recover a viable password, you may have tried to login without creating a new Cisco Security Cloud Sign On account, you need to sign up for a new Cisco Security Cloud Sign On Account by following the instructions in Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication, on page 78.

Login to the Cisco Security Cloud Sign On Dashboard Succeeds but You Can't Launch Security Cloud Control

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control and Cisco Secure Sign-On.

Login Fails Using a Saved Bookmark

Solution You may be attempting to log in using an old bookmark you saved in your browser. The bookmark could be pointing to https://cdo.onelogin.com.

Solution Log in to https://sign-on.security.cisco.com.

- **Solution** If you have not yet created a Cisco Secure Sign-On account, Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication.
- **Solution** If you have created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Security Cloud Control APJ
  - **Solution** Cisco Security Cloud Control Australia
  - **Solution** Cisco Security Cloud Control EU
  - **Solution** Cisco Security Cloud Control India
  - **Solution** Cisco Security Cloud Control US
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Objects

Resolve Duplicate Object Issues

Duplicate objects are two or more objects on the same device with different names but the same values. These objects are usually created accidentally, serve similar purposes, and are used by different policies. After resolving duplicate object issues, Security Cloud Control updates all affected object references with the retained object name.

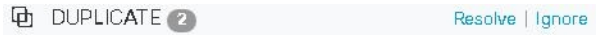
To resolve duplicate object issues:

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Then Object Filters the objects to find duplicate object issues.

Step 3 Select one of the results. In the objects details panel, you will see the DUPLICATE field with the number of duplicates affected:



Step 4 Click **Resolve**. Security Cloud Control displays the duplicate objects for you to compare.

Step 5 Select two of the objects to compare.

Step 6 You now have these options:

- If you want to replace one of the objects with the other, click **Pick** for the object you to keep, click **Resolve** to see what devices and network policies will be affected, and then click **Confirm** if you are satisfied with the changes. Security Cloud Control keeps the object you selected as the replacement and deletes the duplicate.
- If you have an object in the list that you want to ignore, click **Ignore**. If you ignore an object, it will be removed from the list of duplicate objects that Security Cloud Control shows you.
- Click **Ignore All** if you want to keep the object but do not want Security Cloud Control to find it in a search for duplicate objects.

Step 7 Once the duplicate object issue has been resolved Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Resolving Inconsistent or Unused Security Zone Objects

Security zone objects can be marked inconsistent or unused like other objects. See Resolve Unused Object Issues and Resolve Inconsistent Object Issues for instructions on how to resolve these issues.

Related Information:

- Security Zone Object
- Assign a Firepower Interface to a Security Zone
- Deleting Objects

Resolve Unused Object Issues

Unused objects are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule.

Related Information:

- Export a List of Devices and Services, on page 95
- Bulk Reconnect Devices to Security Cloud Control, on page 99

Resolve an Unused Object Issue

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Then Object Filters the objects to find unused object issues.

Step 3 Select one or more unused objects.

Step 4 You now have these options:

- In the Actions pane, click **Remove** to remove the unused object from Security Cloud Control.
- In the Issues pane, click **Ignore.** If you ignore an object, Security Cloud Control will stop displaying it among the results of unused objects objects.

Step 5 If you removed the unused object, Preview and Deploy Configuration Changes for All Devices, on page 568 the changes you made now, or wait and deploy multiple changes at once.

Note To resolve unused object issues in bulk, see Resolve Object Issues in Bulk.

Remove Unused Objects in Bulk

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 Then Object Filters the objects to find unused object issues.

Step 3 Select the unused objects you want to delete:

- Click the checkbox in the object table header row to select all the objects on the page.
- Select individual unused objects in the object table.

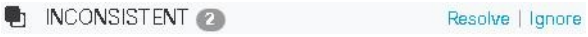
Step 4 In the Actions pane on the right, click **Remove** to remove all the unused objects you selected in Security Cloud Control. You can remove 99 objects at a time.

Step 5 Click **OK** to confirm you want to delete the unused objects.

Step 6 You have two choices to deploy these changes:

- Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- Open the **Inventory** page and find the devices that were affected by the change. Select all the devices affected by the change and, in the **Management** pane, click **Deploy All**. Read the warning and take the appropriate action.

Resolve Inconsistent Object Issues

Inconsistent objects 

are objects with the same name, but different values, on two or more devices. Sometimes users create objects in different configurations with the same name and content, but over time the values of these objects diverge, which creates the inconsistency.

Note: To resolve inconsistent object issues in bulk, see Resolve Object Issues in Bulk.

You can perform the following on inconsistent objects:

- **Ignore:** Security Cloud Control ignores the inconsistency between objects and retains their values. The objects will no longer be listed under the inconsistency category.
- **Merge:** Security Cloud Control combines all selected objects and their values into a single object group.
- **Rename:** Security Cloud Control allows you to rename one of the inconsistent objects and give it a new name.
- **Convert Shared Network Objects to Overrides:** Security Cloud Control allows you to combine inconsistent shared objects (with or without overrides) into a single shared object with overrides. The most common default value from the inconsistent objects is set as a default in the newly formed object.

Note If there are multiple common default values, one of them is selected as the default. The remaining default values and override values are set as overrides of that object.

- **Convert Shared Network Group to Additional Values:** - Security Cloud Control allows you to combine inconsistent shared network groups into a single shared network group with additional values. The criteria for this functionality is that the inconsistent network groups to be converted must have a minimum of one common object with the same value. All default values that match this criterion becomes the default values, and the remaining objects are assigned as additional values of the newly formed network group.

  For example, consider two inconsistent shared network groups. The first network group 'shared_network_group' is formed with 'object_1' (192.0.2.x) and 'object_2' (192.0.2.y). It also contains additional value 'object_3' (192.0.2.a). The second network group 'shared_network_group' is formed with 'object_1' (192.0.2.x) and additional value 'object_4' (192.0.2.b). On converting the shared network group to additional values, the newly formed group 'shared_network_group' contain 'object_1' (192.0.2.x) and 'object_2' (192.0.2.y)' as default values and 'object_3' (192.0.2.a) and 'object_4' (192.0.2.b) as additional values.

Note When you create a new network object, Security Cloud Control auto assigns its value as an override to an existing shared network object with the same name. This is also applicable when a new device is onboarded to Security Cloud Control.

The auto-assignment happens only when the following criteria are met:

1. The new network object must be assigned to a device.
2. Only one shared object with the same name and type must be existing in the tenant.
3. The shared object must already contain overrides.

To resolve inconsistent object issues:

Procedure

Step 1 In the Security Cloud Control navigation bar on the left, click **Objects** and choose an option.

Step 2 Then Object Filters the objects to find inconsistent object issues.

Step 3 Select an inconsistent object. In the objects details panel, you will see the INCONSISTENT field with the number of objects affected:

Step 4 Click **Resolve**. Security Cloud Control displays inconsistent objects for you to compare.

Step 5 You now have these options:

- **Ignore All:**
  a. Compare the objects presented to you and on one of the objects, click **Ignore**. Or, to ignore all objects, click **Ignore All**.
  b. Click **OK** to confirm.
- **Resolve by merging objects:**
  a. Click **Resolve by Merging X Objects**.
  b. Click **Confirm**.
- **Rename:**
  a. Click **Rename**.
  b. Save your changes to affected network policies and devices and click **Confirm**.
- **Convert to Overrides (for inconsistent shared objects):** When comparing shared objects with overrides, the comparison panel shows only the default values in the **Inconsistent Values** field.
  a. Click **Convert to Overrides**. All inconsistent objects will be converted to a single shared object with overrides.

b. Click **Confirm**. You can click **Edit Shared Object** to view the details of the newly formed object. You can use up and down arrows to move the values between default and override.

- **Convert to Additional Values (for inconsistent network groups):**

  a. Click **Convert to Additional Values**. All inconsistent objects will be converted to a single shared object with additional values.

  b. Save your changes to affected network policies and devices and click **Confirm**.

Step 6 After resolving the inconsistencies, Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Resolve Object Issues in Bulk

One way to resolve objects with Resolve Unused Object Issues, Resolve Duplicate Object Issues, or Resolve Inconsistent Object Issues, on page 751 issues is to ignore them. You can select and ignore multiple objects, even if objects exhibit more than one issue. For example, if an object is both inconsistent and unused, you can only ignore one issue type at a time.

Important If the object becomes associated with another issue type at a later time, the ignore action you committed only affects the issues you selected at that time. For example, if you ignored an object because it was a duplicate and the object is later marked inconsistent, ignoring it as a duplicate object does not mean it will be ignored as an inconsistent object.

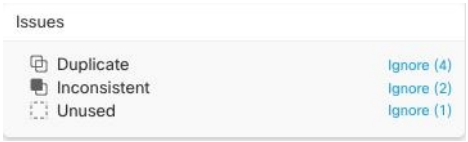
To ignore issues in bulk, follow this procedure:

Procedure

Step 1 In the left pane, click **Objects** and choose an option.

Step 2 To narrow your search, you can Object Filters object issues.

Step 3 In the Object table, select all the applicable objects you want to ignore. The Issues pane groups objects by issue type.



Step 4 Click **Ignore** to ignore issues by type. You must **Ignore** each issue type separately.

Step 5 Click **OK** to confirm you want to ignore those objects.

Device Connectivity States

You can view the connectivity states of the devices onboarded in your Security Cloud Control tenant. This topic helps you understand the various connectivity states. On the **Inventory** page, the **Connectivity** column displays the device connectivity states.

When the device connectivity state is 'Online' it means that the device is powered on and connected to Security Cloud Control. The other states described in the table below usually occur when the device is running into problems for various reasons. The table provides the method to recover from such problems. It may be that there is more than one problem causing the connection failure. When you attempt to reconnect, Security Cloud Control will prompt you to fix all of these problems first before performing the reconnect.

Device Connectivity State	Possible Reasons	Resolution
Online	Device is powered on and connected to Security Cloud Control.	NA
Offline	Device is powered down or lost network connectivity.	Check whether the device is offline.
Insufficient licenses	Device doesn't have sufficient licenses.	Troubleshoot Insufficient Licenses, on page 756
Invalid credentials	Username and password combination used by Security Cloud Control to connect to the device is incorrect.	Troubleshoot Invalid Credentials, on page 756
Onboarding	Device onboarding is initiated but is not complete.	Check you device's connectivity and ensure you complete the device registration.
Pending Setup	Device registration has failed.	Troubleshoot Onboarding a Device to the Cloud-delivered Firewall Management Center Using the CLI Registration Key
New Certificate Detected	Certificate on the device has changed. If the device uses a self-signed certificate, then this could have happened due to the device being power cycled.	Troubleshoot New Certificate Issues, on page 757
Device Unregistered	FDM-managed device has been unregistered from Cloud via FDM.	Troubleshoot Device Unregistered, on page 717

Device Connectivity State	Possible Reasons	Resolution
Claim Error	Security Cloud Control fails to claim the FDM-managed device. Some of the possible reasons could be that an invalid serial number has been entered or the device serial number has already been claimed.	Claim Error
Onboarding Error	Security Cloud Control may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error, on page 765
Provisioning Error	FDM-managed device initial provisioning has failed.	Provisioning Error
Unreachable	• Device is powered down. • IP address has changed on the device. • Device has been deleted from Cisco Cloud.	Troubleshoot Unreachable Connection State, on page 767

Troubleshoot Device Unregistered

The FDM-managed device may have been unregistered from the cloud via Firewall device manager.

Perform the following to register the device again on the cloud:

Procedure

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the **FTD** tab and select the device in the "Device Unregistered" state, and see the error message on the right.

Step 3 If the unregistered device was onboarded using the registration key, Security Cloud Control prompts you to generate a new registration key as the previously applied key has expired.

a) Click the Refresh button to generate a new registration key and then click the Copy icon .
b) Log into the Firewall device manager of the device you want to reregister with Security Cloud Control.
c) Under **System Settings**, click **Cloud Services**.
d) In the Security Cloud Control area, expand **Get Started**.
e) In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.
f) Click **Register** and then **Accept** the Cisco Disclosure. Firewall device manager sends the registration request to Security Cloud Control.
g) Refresh the **Inventory** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
h) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.

Step 4 If the unregistered device was onboarded using the serial number, Security Cloud Control prompts you to auto-enroll the device from Firewall device manager.

a) Log into the Firewall device manager of the device you want to reregister with Security Cloud Control.
b) Under **System Settings**, click **Cloud Services**.
c) Select the **Auto-enroll with Tenancy from Security Cloud Control** option and click **Register**.
d) Refresh the **Inventory** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
e) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.

Troubleshoot Insufficient Licenses

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.
- If the device status doesn't change, refresh the Security Cloud Control portal by signing out from Security Cloud Control and signing back to resolve any network communication glitch between license server and device.
- If the portal refresh doesn't change the device status, perform the following:

Procedure

Step 1 Generate a new token from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab and select the device with the **Insufficient License** state.

Step 5 In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.

Step 6 In the **Activate** field, paste the new token and click **Register Device**.

Once the token is applied successfully to the device, its connectivity state turns to **Online**.

Troubleshoot Invalid Credentials

Perform the following to resolve device disconnection due to invalid credentials:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the device with the **Invalid Credentials** state.

Step 4 In the **Device Details** pane, click **Reconnect** appearing in **Invalid Credentials**. Security Cloud Control attempts to reconnect with your device.

Step 5 When prompted enter the new username and password for the device.

Step 6 Click **Continue**.

Step 7 After the device is online and ready to use, click **Close**.

Step 8 It is likely that because Security Cloud Control attempted to use the wrong credentials to connect to the device, the username and password combination Security Cloud Control should use to connect to the device was changed directly on the device. You may now see that the device is "Online" but the configuration state is "Conflict Detected." Use Resolve Configuration Conflicts to review and resolve configuration differences between Security Cloud Control and the device.

Troubleshoot New Certificate Issues

Security Cloud Control's Use of Certificates

Security Cloud Control checks the validity of certificates when connecting to devices. Specifically, Security Cloud Control requires that:

1. The device uses a TLS version equal to or greater than 1.0.
2. The certificate presented by the device is not expired, and its issuance date is in the past (i.e. it is already valid, not scheduled to become valid at a later date).
3. The certificate must be a SHA-256 certificate. SHA-1 certificates will not be accepted.
4. One of these conditions is true:
   - The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.
   - The device uses a certificate signed by a trusted Certificate Authority (CA), and provides a certificate chain linking the presented leaf certificate to the relevant CA.

These are the ways Security Cloud Control uses certificates differently than browsers:

- In the case of self-signed certificates, Security Cloud Control overrides the domain name check, instead checking that the certificate exactly matches the one trusted by an authorized user during device onboarding or reconnection.
- Security Cloud Control does not yet support internal CAs. There is currently no way to check a certificate signed by an internal CA.

  It is possible to disable certificate checking for ASA devices on a per-device basis. When an ASA's certificate cannot be trusted by Security Cloud Control, you will have the option of disabling certificate checking for that device. If you have attempted to disable certificate checking for the device and you are still unable to onboard it, it is likely that the IP address and port you specified for the device is incorrect or unreachable. There is no way to disable certificate checking globally, or to disable certificate checking for a device with a supported certificate. There is no way to disable certificate checking for non-ASA devices.

When you disable certificate checking for a device, Security Cloud Control will still use TLS to connect to the device, but it will not validate the certificate used to establish the connection. This means that a passive man-in-the-middle attacker will not be able to eavesdrop on the connection, but an active man-in-the-middle could intercept the connection by supplying Security Cloud Control with an invalid certificate.

Identifying Certificate Issues

There are several reasons that Security Cloud Control may not be able to onboard a device. When the UI shows a message that "Security Cloud Control cannot connect to the device using the certificate presented," there is a problem with the certificate. When the UI does not show this message, the problem is more likely related to connectivity problems (the device is unreachable) or other network errors.

To determine why Security Cloud Control rejects a given certificate, you can use the openssl command-line tool on the SDC host or another host that can reach the relevant device. Use the following command to create a file showing the certificates presented by the device:

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

This command will start an interactive session, so you will need to use Ctrl-c to exit after a couple of seconds.

You should now have a file containing output like the following:

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
```

```
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

The first thing to note in this output is the last line, where you see the **Verify return code**. If there is a certificate issue, the return code will be non-zero and there will be a description of the error.

Expand this list of certificate error code to see common errors and how to remediate them

0 X509_V_OK The operation was successful.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT The issuer certificate of an untrusted certificate could not be found.

3 X509_V_ERR_UNABLE_TO_GET_CRL The CRL of a certificate could not be found.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. This is only meaningful for RSA keys.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE The CRL signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. Unused.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY The public key in the certificate SubjectPublicKeyInfo could not be read.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE The signature of the certificate is invalid.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE The signature of the certificate is invalid.

9 X509_V_ERR_CERT_NOT_YET_VALID The certificate is not yet valid: the notBefore date is after the current time. See Verify return code: 9 (certificate is not yet valid) below for more information.

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired; that is, the notAfter date is before the current time. See Verify return code: 10 (certificate has expired) below for more information.

11 X509_V_ERR_CRL_NOT_YET_VALID The CRL is not yet valid.

12 X509_V_ERR_CRL_HAS_EXPIRED The CRL has expired.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD The certificate notBefore field contains an invalid time.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD The certificate notAfter field contains an invalid time.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD The CRL lastUpdate field contains an invalid time.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD The CRL nextUpdate field contains an invalid time.

17 X509_V_ERR_OUT_OF_MEM An error occurred trying to allocate memory. This should never happen.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN The certificate chain could be built up using the untrusted certificates but the root could not be found locally.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE No signatures could be verified because the chain contains only one certificate and it is not self-signed. See "Verify return code: 21 (unable to verify the first certificate)" below for more information. Verify return code: 21 (unable to verify the first certificate) below for more information.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG The certificate chain length is greater than the supplied maximum depth. Unused.

23 X509_V_ERR_CERT_REVOKED The certificate has been revoked.

24 X509_V_ERR_INVALID_CA A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED The basicConstraints pathlength parameter has been exceeded.

26 X509_V_ERR_INVALID_PURPOSE The supplied certificate cannot be used for the specified purpose.

27 X509_V_ERR_CERT_UNTRUSTED The root CA is not marked as trusted for the specified purpose.

28 X509_V_ERR_CERT_REJECTED The root CA is marked to reject the specified purpose.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.

30 X509_V_ERR_AKID_SKID_MISMATCH The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH The current candidate issuer certificate was rejected because its issuer name and serial number were present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.

50 X509_V_ERR_APPLICATION_VERIFICATION An application specific error. Unused.

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, Security Cloud Control may generate a "New Certificate Detected" message as both a **Configuration Status** and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Note When you Bulk Reconnect Devices to Security Cloud Control more than one managed device to Security Cloud Control at the same time, Security Cloud Control automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Use the following procedure to resolve a new certificate:

1. In the left pane, click **Security Devices**.
2. Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.
3. In the action pane, click **Review Certificate**. Security Cloud Control allows you to download the certificate for review and accept the new certificate.
4. In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

   Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

Certificate Error Codes

Verify return code: 0 (ok) but Security Cloud Control returns certificate error

Once Security Cloud Control has the certificate, it attempts to connect to the URL of the device by making a GET call to "https://<device_ip>:<port>". If this does not work, Security Cloud Control will display a certificate error. If you find that the certificate is valid (openssl returns 0 ok) the problem may be that a different service is listening on the port you're trying to connect to. You can use the command:

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

to determine whether you are definitely talking to an ASA and check if HTTPS server running on the correct port on the ASA:

```
 # show asp table socket
Protocol         Socket         State         Local Address             Foreign Address
SSL             00019b98         LISTEN        192.168.1.5:443             0.0.0.0:*
SSL             00029e18         LISTEN        192.168.2.5:443             0.0.0.0:*
TCP             00032208         LISTEN        192.168.1.5:22              0.0.0.0:*
```

Verify return code: 9 (certificate is not yet valid)

This error means that the issuance date of the certificate provided is in the future, so clients will not treat it as valid. This can be caused by a poorly-constructed certificate, or in the case of a self-signed certificate it can be cause by the device time being wrong when it generated the certificate.

You should see a line in the error including the notBefore date of the certificate:

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

From this error, you can determine when the certificate will become valid.

Remediation

The notBefore date of the certificate needs to be in the past. You can reissue the certificate with an earlier notBefore date. This issue can also arise when the time is not set correctly either on the client or issuing device.

Verify return code: 10 (certificate has expired)

This error means that at least one of the certificates provided has expired. You should see a line in the error including the notBefore date of the certificate:

```
 error 10 at 0 depth lookup:certificate has expired
```

The expiration date is located in the certificate body.

Remediation

If the certificate is truly expired, the only remediation is to get another certificate. If the certificate's expiration is still in the future, but openssl claims that it is expired, check the time and date on your computer. For instance, if a certificate is set to expire in the year 2020, but the date on your computer is in 2021, your computer will treat that certificate as expired.

Verify return code: 21 (unable to verify the first certificate)

This error indicates that there is a problem with the certificate chain, and openssl cannot verify that the certificate presented by the device should be trusted. Let's look at the certificate chain from the example above to see how certificate chains should work:

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
```

```
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

The certificate chain is a list of certificates presented by the server, beginning with the server's own certificate and then including increasingly higher-level intermediate certificates linking the server's certificate with a Certificate Authority's top-level certificate. Each certificate lists its Subject (the line starting with 's:' and its Issuer (the line starting with 'i').

The Subject is the entity identified by the certificate. It includes the Organization name and sometimes the Common Name of the entity for which the certificate was issued.

The Issuer is the entity that issued the certificate. It also includes an Organization field and sometimes a Common Name.

If a server had a certificate issued directly by a trusted Certificate Authority, it would not need to include any other certificates in its certificate chain. It would present one certificate that looked like:

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

Given this certificate, openssl would verify that the ExampleCo certificate for ***.example.com** was correctly signed by the Trusted Authority certificate, which would be present in openssl's built-in trust store. After that verification, openssl would successfully connect to the device.

However, most servers do not have certificates signed directly by a trusted CA. Instead, as in the first example, the server's certificate is signed by one or more intermediates, and the highest-level intermediate has a certificate signed by the trusted CA. OpenSSL does not trust these intermediate CAs by default, and can only verify them if it is given a complete certificate chain ending in a trusted CA.

It is critically important that servers whose certificates are signed by intermediate authorities supply ALL the certificates linking them to a trusted CA, including all of the intermediate certificates. If they don't supply this entire chain, the output from openssl will look something like this:

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
```

```
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

This output shows that the server only provided one certificate, and the provided certificate was signed by an intermediate authority, not a trusted root. The output also shows the characteristic verification errors.

Remediation

This problem is caused by a misconfigured certificate presented by the device. The only way to fix this so that Security Cloud Control or any other program can securely connect to the device is to load the correct certificate chain onto the device, so that it will present a complete certificate chain to connecting clients.

To include the intermediate CA to the trustpoint follow one of the links below (depending on your case - if CSR was generated on the ASA or not):

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, Security Cloud Control may generate a "New Certificate Detected" message as both a **Configuration**

Status and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Note When you Bulk Reconnect Devices to Security Cloud Control more than one managed device to Security Cloud Control at the same time, Security Cloud Control automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Use the following procedure to resolve a new certificate:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.

Step 5 In the action pane, click **Review Certificate**. Security Cloud Control allows you to download the certificate for review and accept the new certificate.

Step 6 In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

Troubleshoot Onboarding Error

The device onboarding error can occur for various reasons.

You can take the following actions:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the appropriate device type tab and select the device running into this error. In some cases, you will see the error description on the right. Take the necessary actions mentioned in the description.

Or

Step 3 Remove the device instance from Security Cloud Control and try onboarding the device again.

Resolve the Conflict Detected Status

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 576 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Note For an On-Premises Firewall Management Center, click **Administration** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.

Step 5 In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

- The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
- The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

Step 6 Resolve the conflict by selecting one of the following:

- **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

  Note As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

Note All configuration changes, rejected or accepted, are recorded in the change log.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Note For an On-Premises Firewall Management Center, click **Administration** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reported as Not Synced.

Step 5 In the **Not synced** panel to the right, select either of the following:

- **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

Troubleshoot Unreachable Connection State

The device may be in "unreachable" for various reasons:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab and select the device in the **Unreachable** state.

Step 4 Click **Reconnect.**

Step 5 Take one of these actions based on the message appearing on the right:

a. If you have onboarded the FDM-managed device using the IP address and device credentials, the following message appears:

"*This device is unreachable, review the IP address and port*," enter the new IP address and/or new port information of the device in the message box. It is likely that because Security Cloud Control attempted to connect to an invalid IP address, the IP address for the device was changed directly on the device.

Note If the device was rebooted, and there are no other pending changes, the device should return to an online connection state, and no further action is needed.

You may now see that the device is "Online", but the configuration state is "Conflict Detected." Use Resolve Configuration Conflicts, to review the configuration differences between Security Cloud Control and the device.

b. If you are onboarding the FDM-managed device using the registration token or serial number, the following message appears:

"*This device has been deleted from Cisco Cloud. The deletion could be caused as part of the Return Material Authorization (RMA) process*". It means that the faulty device that you have returned to the RMA team has been deleted from Cisco Cloud as a part of the RMA process.

As a result, you'll see that the device Connectivity status is "Unreachable" in Security Cloud Control.

- For the RMA case, you need to perform the following steps in Security Cloud Control:

  1. If the device was successfully onboarded, you need to save the device configuration as a template. See Configure an FDM Template.

     Remove the device instance from Security Cloud Control.

  2. Power on the new replacement device that you have received from the RMA team and onboard it to Security Cloud Control. See Onboard an FDM-Managed Device using the Device's Serial Number.

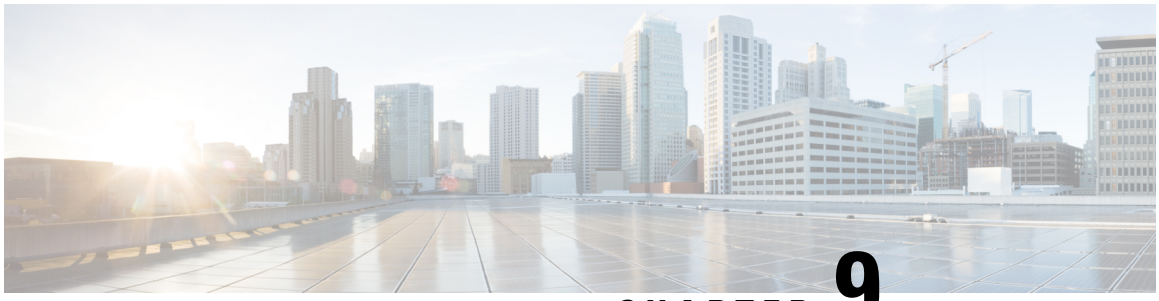
     Important The replacement device will probably have a different serial number and needs to be onboarded as a new device.

     You'll now see that the device is "Online", but the configuration state is "Conflict Detected."

  3. Use Resolve Configuration Conflicts, to review the configuration differences between Security Cloud Control and the device.

     Apply the previously saved template to the new device. See Apply an FDM Template.

- If you have sold the device or transferred its ownership to another user outside of your tenant without erasing the device's configuration, you will no longer possess the device. This error occurs when the buyer reimages the device. If the device was configured correctly and synced earlier, you can save the device configuration as a template and then remove the device instance from Security Cloud Control.



CHAPTER 9

FAQ and Support

This chapter contains the following sections:

Cisco Security Cloud Control

What is Cisco Security Cloud Control?

Cisco Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that allows network administrators to create and maintain consistent security policies across various security devices.

You can use Security Cloud Control to manage these devices:

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Umbrella
- Meraki
- Cisco IOS devices
- Amazon Web Services (AWS) instances
- Devices administered using an SSH connection

Security Cloud Control administrators can monitor and maintain all these device types through a single interface.

FAQ About Onboarding Devices to Security Cloud Control

FAQs About Onboarding Secure Firewall ASA to Security Cloud Control

How do I onboard an ASA using credentials?

You can onboard ASAs one at a time or in a bulk operation. device at a time. When onboarding an ASA that is part of a high-availability pair, use Onboard an ASA Device to onboard only the primary device of the pair. The method of onboarding a security context or admin context is the same for onboarding any other ASA.

How do I onboard more than one ASA at a time?

You can create a list of ASAs using a CSV file, and Security Cloud Control will onboard all the ASAs in the list. See Onboard ASAs in Bulk for instructions on how to bulk onboard ASAs.

What do I do after onboarding my ASAs?

See Managing ASA with Cisco Security Cloud Control to get started.

FAQs About Onboarding FDM-Managed Devices to Security Cloud Control

How do I onboard FDM-managed devices?

There are different methods of onboarding an FDM-managed device. We recommend using the registration key method. See Onboard an FDM-Managed Device to get started.

FAQs About Onboarding Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center

How do I onboard Secure Firewall Threat Defense?

You can onboard an FTD device using a CLI registration key, through zero-touch provisioning, or with a serial number.

What do I do after onboarding my Secure Firewall Threat Defense?

Once the device is sychronized, navigate to Tools & Services > Firewall Management Center and select an action from the Actions, Management, or Settings pane to begin configuring your threat defense device in cloud-delivered Firewall Management Center. See Cloud-delivered Firewall Management Center Application Page to get started.

How do I troubleshoot my Secure Firewall Threat Defense?

See Troubleshoot Onboarding your Secure Firewall Threat Defense.

FAQs About On-Premises Secure Firewall Management Center

How do I onboard an On-Prem management center?

You can onboard an On-Prem Management Center to Security Cloud Control. Onboarding an On-Prem Management Center also onboards all of the devices registered to the On-Prem Management Center. Security Cloud Control does not support creating or modifying objects or policies associated with the On-Prem Management Center or the devices registered to the On-Prem Management Center. You must make these changes in the On-Prem Management Center UI. See Onboard an On-Prem Management Center to get started.

FAQs About Onboarding Meraki Devices to Security Cloud Control

How do I onboard a Meraki device?

MX devices can be managed by both Security Cloud Control and the Meraki dashboard. Security Cloud Control deploys configuration changes to the Meraki dashboard, which in turn deploys the configuration securely to the device. See Onboard Meraki MX Devices to get started.

FAQs About Onboarding SSH Devices to Security Cloud Control

How do I onboard an SSH device?

You can use the username and password of a highly privileged user stored on the SSH device to onboard the device with a Secure Device Connector (SDC). See Onboard an SSH Device to get started.

How do I delete a device?

You can delete a device from the **Security Devices** page.

FAQs About Onboarding IOS Devices to Security Cloud Control

How do I onboard a Cisco IOS device?

You can onboard a live Cisco device running Cisco IOS (Internetwork Operating System) with a Secure Device Connector (SDC). See Onboard a Cisco IOS Device to get started.

How do I delete a device?

You can delete a device from the **Security Devices** page.

Device Types

What is an Adaptive Security Appliance (ASA)?

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality in one device as well as integrated services with add-on modules. The ASA includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), clustering (combining multiple firewalls into a single

firewall), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPsec VPN, SSL VPN, and clientless SSL VPN support, and many more features. ASAs can be installed on virtual machines or supported hardware.

What is an ASA Model?

An ASA model is a copy of the running configuration file of an ASA device that you have onboarded to Security Cloud Control. You can use an ASA model to analyze the configuration of an ASA device without onboarding the device itself.

What is Firepower Threat Defense (FTD)

Cisco's next generation firewall software image. It strives to combine the best of Sourcefire next generation firewall services and the ASA platform. It can be installed on a number of different Firepower hardware devices or virtual machines. This is not the same as a ASA FirePOWER module. See Devices, Software, and Hardware Supported by Security Cloud Control for more information.

What is Firepower Device Manager (FDM)

Firepower Device Manager is Firepower Threat Defense management software delivered with the FTD image. FDM is designed to manage the one FTD it is delivered with. You may also hear FDM referred to as the "local device manager."

What is Firepower?

Firepower is a general term that refers to a group of next generation firewall hardware and software.

When is a device Synced?

When the configuration on Security Cloud Control and the configuration stored locally on the device are the same.

When is a device Not Synced?

When the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device.

When is a device in a Conflict Detected state?

When the configuration on the device was changed outside of Security Cloud Control (out-of-band), and is now different than the configuration stored on Security Cloud Control.

What is an out-of-band change?

When a change is made to the device outside of Security Cloud Control. The change is made directly on the device using CLI command or by using the on-device manager such as ASDM or FDM. An out-of-band change causes Security Cloud Control to report a "Conflict Detected" state for the device.

What does it mean to deploy a change to a device?

After you onboard a device to Security Cloud Control, Security Cloud Control maintains a copy of its configuration. When you make a change on Security Cloud Control, Security Cloud Control makes a change to its copy of the device's configuration. When you "deploy" that change back to a device, Security Cloud Control copies the changes you made to the device's copy of its configuration. See these topics:

- Preview and Deploy Configuration Changes for All Devices, on page 568
- Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device

What ASA commands are currently supported?

All commands. Click the **Command Line Interface** link under Device Actions to use the ASA CLI.

Are there any scale limitations for device management?

Security Cloud Control's cloud architecture allows it to scale to thousands of devices.

Does Security Cloud Control manage Cisco Integrated Services Routers and Aggregation Services Routers?

Security Cloud Control allows you to create a model device for ISRs and ASRs and import its configuration. You can then create templates based on the imported configurations and export the configuration as a standardized configuration that can be deployed to new or existing ISR and ASR devices for consistent security.

Can Security Cloud Control manage SMA?

No, Security Cloud Control does not currently manage SMA.

Security

Is Security Cloud Control Secure?

Security Cloud Control offers end-to-end security for customer data through the following features:

- Initial Login to Your New Security Cloud Control Tenant, on page 8
- Authentication calls for APIs and database operations
- Data isolation in flight and at rest
- Separation of roles

Security Cloud Control requires multi-factor authentication for users to connect to their cloud portal. Multi-factor authentication is a vital function needed to protect the identity of customers.

All data, in flight and at rest, is encrypted. Communication from devices on customer premises and Security Cloud Control is encrypted with SSL, and all customer-tenant data volumes are encrypted.

Security Cloud Control's multi-tenant architecture isolates tenant data and encrypts traffic between databases and application servers. When users authenticate to gain access to Security Cloud Control, they receive a token. This token is used to fetch a key from a key-management service, and the key is used to encrypt traffic to the database.

Security Cloud Control provides value to customers quickly while making sure customer credentials are secured. This is achieved by deploying a "Secure Data Connector" in the cloud or a customer's own network (in roadmap) that controls all inbound and outbound traffic to make sure the credential data doesn't leave the customer premises.

I received the error "Could not validate your OTP" when logging into Security Cloud Control for the first time

Check that your desktop or mobile device clock is synchronized with a world time server. Clocks being out of sync by less or more than a minute can cause incorrect OTPs to be generated.

Is my device connected directly to Security Cloud Control cloud platform?

Yes. The secured connection is performed using the Security Cloud Control SDC which is used as a proxy between the device and Security Cloud Control platform. Security Cloud Control architecture, designed with security first in mind, enables having complete separation between data traversing back and forth to the device.

How can I connect a device which does not have a public IP address?

You can leverage Security Cloud Control Secure Device Connector which can be deployed within your network and doesn't need any outside port to be open. Once the SDC is deployed you can onboard devices with internal (non-internet routable) IP addresses.

Does the SDC require any additional cost or license?

No.

How can I check the tunnel status? State options

Security Cloud Control performs the tunnel connectivity checks automatically every hour, however ad-hoc VPN tunnel connectivity checks can be performed by choosing a tunnel and requesting to check connectivity. Results may take several seconds to process.

Can I search a tunnel based on the device name as well as its IP address of one of its peers?

Yes. Search and pivot to a specific VPN tunnel details by using available filters and search capabilities on both name and the peers IP addresses.

Troubleshooting

While performing complete deploy of device configuration from Security Cloud Control to managed device, I get a warning "Cannot deploy changes to device". What can I do to solve that?

If an error occurrs when you deploy a full configuration (changes performed beyond Security Cloud Control supported commands) to the device, click "Check for changes" to pull the latest available configuration from device. This may solve the problem and you will be able to continue making changes on Security Cloud Control and deploy them. In case the issue persist, please contact Cisco TAC from the **Contact Support** page.

While resolving out-of-band issue (changes performed outside of Security Cloud Control; directly to a device), comparing the configuration present in Security Cloud Control that of the device, Security Cloud Control presents additional metadata that were not added or modified by me. Why?

As Security Cloud Control expands its functionality, additional information will be collected from the device's configuration to enrich and maintain all required data for better policy and device management analysis. These are not changes that occurred on managed device but already existing information. Resolving the conflict detected state can be easily solved by checking for changes from the device and reviewing the changes occurred.

Why is Security Cloud Control rejecting my certificate?

See Troubleshoot New Certificate Issues

Terminologies and Definitions used in Zero-Touch Provisioning

- **Claimed** - Used in the context of serial number onboarding in Security Cloud Control. A device is "claimed" if its serial number has been onboarded to a Security Cloud Control tenant.
- **Parked** - Used in the context of serial number onboarding in Security Cloud Control. A device is "parked" if it has connected to the Cisco Cloud, and a Security Cloud Control tenant has not claimed its serial number.
- **Initial provisioning** - Used in the context of the initial FTD setup. During this phase, the device accepts EULA, creates a new password, configures management IP address, sets FQDN, sets DNS servers, and chooses to manage the device locally with FDM.
- **Zero-Touch Provisioning** - It is the process of shipping an FTD from the factory to a customer site (typically a branch office), an employee at the site connects the FTD to their network, and the device contacts the Cisco Cloud. At that point, the device is onboarded to Security Cloud Control tenant if its serial number has already been "claimed," or the FTD is "parked" in the Cisco cloud until a Security Cloud Control tenant claims it.

Policy Optimization

How can I identify a case when two or more access lists (within the same access group) are shadowing each other?

Security Cloud Control Network Policy Management (NPM) is able to identify and alert the user if within a rule set, a rule higher in order, is shadowing a different rule. User can either navigate between all network policies or filter to identify all shadow issues.

Note Security Cloud Control supports only fully shadowed rules.

Connectivity

The Secure Device Connector changed IP address, but this was not reflected within Security Cloud Control. What can I do to reflect the change?

In order to obtain and update the new Secure Device Connector (SDC) within Security Cloud Control, you will need to restart the container using the following commands:

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh restartSDC
 <tenant-name>
```

What happens if the IP address used by Security Cloud Control to manage my devices (FTD or ASA) changes?

If the IP address of the device changes for any reason, whether it is a change in the static IP address or a change in the IP address due to DHCP, you can change the IP address that Security Cloud Control uses to connect to the device (see Changing a Device's IP Address in Security Cloud Control, on page 93) and then reconnect the device (see Bulk Reconnect Devices to Security Cloud Control, on page 99). When reconnecting the device you will be asked to enter the new IP address of the device as well as re-enter the authentication credentials.

What networking is required to connect my ASA to Security Cloud Control?

- ASDM image present and enabled for ASA.
- Public interface access to 52.25.109.29, 52.34.234.2, 52.36.70.147
- ASA's HTTPS port must be set to 443 or to a value of 1024 or higher. For example, it cannot be set to port 636.
- If the ASA under management is also configured to accept AnyConnect VPN Client connections, the ASA HTTPS port must be changed to a value of 1024 or higher.

Complete the Initial Configuration of a Secure Firewall Threat Defense Device Using the CLI

Connect to the device's CLI to perform initial setup, including setting the management IP address, gateway, and other basic networking settings using the setup wizard. Ensure all DNS and firewall ports are accessible for communication.

The dedicated management interface is a special interface with its own network settings. If you do not want to use the management interface, you can use the CLI to configure a data interface instead.

This configuration is ideal for devices that are going to be onboarded with their CLI registration key.

Note Do **not** use this configuration procedure for devices that are onboarding with zero-touch provisioning.

Procedure

Step 1 Connect to the device's CLI, either from the console port or using SSH to the management interface. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

(Firepower and Secure Firewall hardware models) The console port connects to the FXOS CLI. The SSH session connects directly to the threat defense CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

(Firepower and Secure Firewall hardware models) At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default.

For Firepower and Secure Firewall hardware, see the Reimage Procedures in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Threat Defense .

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3 (Firepower and Secure Firewall hardware models) If you connected to FXOS on the console port, connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to the device, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the threat defense command reference.

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

Note The management interface settings are used even when you enable threat defense access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—If you want to use a data interface for threat defense access instead of the management interface, choose **manual**. Although you do not plan to use the management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.

- **Enter the IPv4 default gateway for the management interface**—If you want to use a data interface for threat defense access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the FMC access data interface.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **YES** to configure the device for the device to be managed by either the cloud-delivered Firewall Management Center or Secure Firewall device manager.

  Manage the device locally?—Enter **NO** to configure the device for remote management with the on-premises management center.
- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface threat defense access is only supported in routed firewall mode.

Step 5 (Optional) Configure a data interface for management center access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command. See About Data Interfaces, on page 780 for more informatio.

- The original management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the management interface gateway to **data-interfaces**, this command will set it now.
- When you onboard the device for threat defense management through Security Cloud Control, Security Cloud Control discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. You can later make changes to the access interface configuration, but make sure you don't make changes that can prevent the device or Security Cloud Control from re-establishing the management connection. If the management connection is disrupted, the device includes the **configure policy rollback** command to restore the previous deployment.
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  Also, local DNS servers are only retained if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in Security Cloud Control, including the DNS servers, to match the device configuration.
- You can change the management interface after you onboard the threat defense for threat defense management through threat defense, to either the management interface or another data interface.

- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 6 (Optional) Limit data interface access to Security Cloud Control on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

About Data Interfaces

You can use either the dedicated management interface or a regular data interface for communication with the device. Security Cloud Control access on a data interface is useful if you want to manage the FTD remotely from the outside interface, or you do not have a separate management network. Security Cloud Control supports high availability on the FTD managed remotely from the data interface.

FTD management access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using Security Cloud Control. Because the management interface gateway will be changed to be the data interfaces, you also cannot SSH to the management interface from a remote network unless you add a static route for the management interface using the **configure network static-routes** command.

How Security Cloud Control Processes Personal Information

To learn how Security Cloud Control processes your personal identifiable information, see the Cisco Security Cloud Control Privacy Data Sheet.

Contact Security Cloud Control Support

This chapter covers the following sections:

Export The Workflow

We strongly recommend exporting the workflow of a device that is experience issues prior to opening a support ticket. This additional information can help the support team expeditiously identify and correct any troubleshooting efforts.

Use the following procedure to export the workflow:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab and select the device you need to troubleshoot.

Use the **filter** or **search bar** to locate the device you need to troubleshoot. Select the device so it is highlighted.

Step 4 In the **Device Actions** pane, select **Workflows**.

Step 5 Click the **Export** button located at the top right of the page, above the table of events. The file automatically saves locally as a **.json** file. Attach this to any emails or tickets you open with TAC.

Open a Support Ticket with TAC

A customer using a 30-day trial or a licensed Security Cloud Control account can open a support ticket with Cisco's Technical Assistance Center (TAC).

- How Security Cloud Control Customers Open a Support Ticket with TAC.
- How Security Cloud Control Trial Customers Open a Support Ticket with TAC.

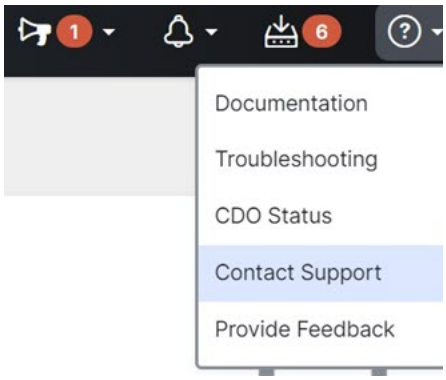
How Security Cloud Control Customers Open a Support Ticket with TAC

This section explains how a customer using a licensed Security Cloud Control tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 Next to your tenant name, click the help button and select **Contact Support**.



Step 3 Click **Support Case Manager**.

Step 4 Click the blue **Open New Case** button.

Step 5 Click **Open Case**.

Step 6 Select **Products and Services** and then click **Open Case**.

Step 7 Choose a **Request Type**.

Step 8 Expand **Find Product by Service Agreement** row.

Step 9 Fill in all the fields. Many of the fields are obvious. This is some additional information:

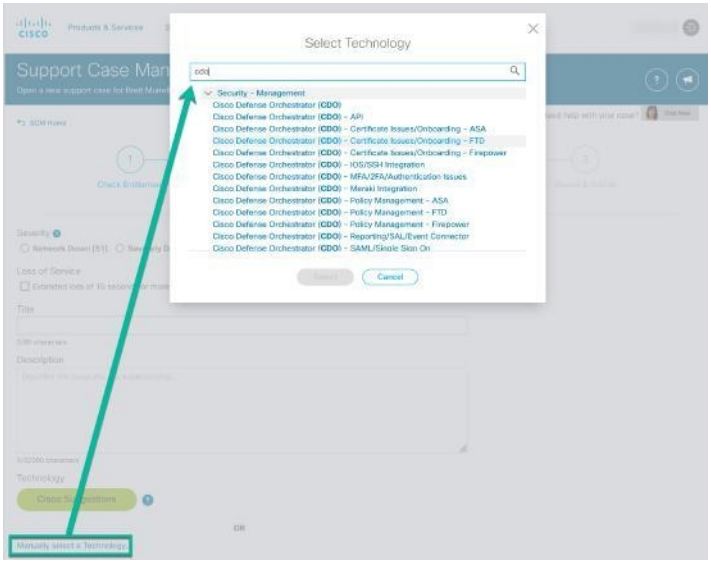
- **Product Name (PID)** - If you no longer have this number, see the Cisco Security Cloud Control Data Sheet.
- **Product Description** - This is the description of the PID.
- **Site Name** - Enter your site name. If you are a Cisco Partner opening a case for one of your customers, enter the customer's name.
- **Service Contract** - Enter your service contract number.
  - **Important**: In order for your case to be associated with your Cisco.com account, you need to associate your contract number to your Cisco.com profile. Use this procedure to associate your contract number to your Cisco.com profile.
    a. Open to Cisco Profile Manager.
    b. Click the **Access Management** tab.
    c. Click **Add Access**.
    d. Choose **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com** and click **Go**.
    e. Enter service contracts number(s) in the space provided and click **Submit**. You will receive notification via email that the service contract associations have been completed. Service contract association can take up to 6 hours to complete.

Important Important: If you are not able to access any of the links below, please contact your authorized Cisco partner or re-seller, your Cisco account representative, or the individual in your company who manages Cisco service agreement information.

Step 10 Click **Next.**

Step 11 In the **Describe Problem** screen, scroll down to **Manually select a Technology**, click it, and type **Security Cloud Control** in the search field.

Step 12 Select the category that best matches your request, and click **Select**.



Step 13 Complete the remainder of the service request and click **Submit**.

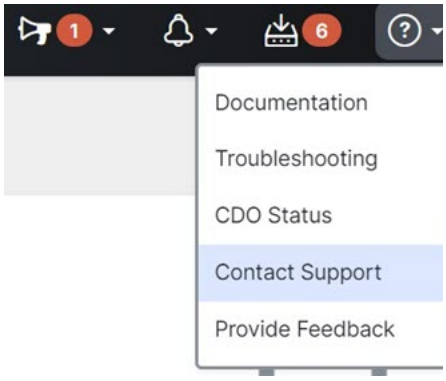
How Security Cloud Control Trial Customers Open a Support Ticket with TAC

This section explains how a customer using a free trial of a Security Cloud Control tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 Next to your tenant and account name, click the help button and select **Contact Support**.



Step 3 In the **Enter Issue or request below** field, specify the issue that you are facing or your request and click **Submit**.

Your request, along with the technical information, will be sent to the support team, and a technical support engineer will respond to your query.

Security Cloud Control Service Status Page

Security Cloud Control maintains a customer-facing service status page that shows you if the Security Cloud Control service is up and any service interruptions it may have had. You can view up-time information with daily, weekly, or monthly graphs.

You can reach the Security Cloud Control status page by clicking **Security Cloud Control Status** in the help menu on any page in Security Cloud Control.

On the status page, you can click the **Subscribe to Updates** to receive a notification if the Security Cloud Control service goes down.