Managing ASA with Cisco Defense Orchestrator

First Published: 2021-03-10

Last Modified: 2024-10-04

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

Managing ASA with Cisco Defense Orchestrator

Managing ASA with Cisco Defense Orchestrator

Cisco Defense Orchestrator (CDO) is a cloud-based, multi-device manager that provides a simple, consistent, and secure way of managing security policies on all your ASA devices.

The goal of this document is to provide customers new to CDO with an outline of activities you can use to standardize objects and policies, upgrade managed devices, and manage VPN policies and monitor remote workers. This document assumes the following:

- You have opened a 30-day trial account or you have purchased CDO and Cisco has created a CDO tenant for you.
- You have set up an Initial Login to Your New CDO Tenant, on page 3 for your User Roles in CDO user.
- Your ASAs are already configured and you are using it in your enterprise.
- If the ASA you want CDO to manage cannot be directly accessed from the internet, then you will need to deploy a Secure Device Connector (SDC) in your network. The SDC manages the communication between CDO and your ASA. See Deploy a Secure Device Connector Using CDO's VM Image, on page 11 or Deploy a Secure Device Connector On Your VM, on page 15 for more information.

Get Started

Secure Device Connectors

When using device credentials to connect CDO to your ASA, it is a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between CDO and the ASA. ASAs can all be onboarded to CDO using device credentials. If you do not want the SDC to manage communications between your ASA and CDO, and your device can be accessed directly from the internet, you do not need to install an SDC in your network. Your ASAs can be onboarded to CDO using the cloud Connector.

Deploying more than one SDC for your tenant allows you to manage more devices with your CDO tenant 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. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices.

To view SDC:

1. Log in to CDO.
2. From the CDO menu, choose **Admin** > **Secure Connectors**.

Onboard Devices

You can onboard your ASAs to CDO in Onboard Multiple ASAs to CDO or Onboard ASA Device to CDO. See ASA Support Specifics for a discussion of ASA software and hardware supported by CDO.

Create Additional CDO Users on your Tenant

There are a variety of user roles in CDO: Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a CDO user has access to more than one tenant, they may have the same user ID but different roles on different tenants. 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. See User Roles in CDO, on page 70 to learn about the privileges granted to different types of users.

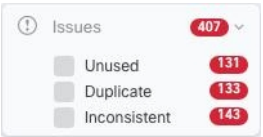
When your tenant was created, you were automatically assigned a Super Admin user. The Super Admin has the ability to create other users on your tenant. For those new users to connect to the tenant, they need to have, or create, a Cisco Secure Sign-On account with the same email address as their user record in CDO. See Add a User Account to CDO, on page 74 to create a user record in CDO.

Policy Orchestration

Policy orchestration involves reviewing objects and policies. Keep in mind when you are working with ASA policies that CDO refers to "access-groups" as "access policies." When you look for ASA access policies you navigate from the CDO menu bar Policies > ASA Access Policies.

Resolve Network Object Issues

Over the years, you may have objects on your security device that are no longer used, are duplicates of other objects, or whose values are inconsistent across devices. Begin your orchestration task by fixing these object issues.



Address object issues in a the order below. The work you do in the early steps may resolve the number of issues you have to address in later steps:

1. Resolve an Unused Object Issue. Unused objects, are objects that exist in a device but are not referenced by another object, an access-list, or a NAT rule.
2. 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,

Managing ASA with Cisco Defense Orchestrator

and are used by different policies. After resolving duplicate object issues, CDO updates all affected object references with the retained object name.

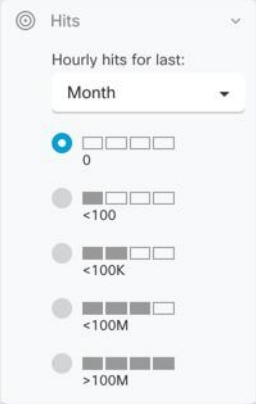
3. Resolve Inconsistent Object Issues. Inconsistent objects are objects with the same name, but different values, on two or more devices. Sometimes users create objects in different configurations with the same name and content, but over time the values of these objects diverge, which creates the inconsistency. This could be a security issue. You may have a rule that is protecting an outdated resource.

Fix Shadow Rules

Now that you have resolved your network object issues, review network policies for Shadowed Rules and fix them. A **shadow rule** is marked by a half-moon badge on the ASA access policies page. The rules in an access policy are configured in a list and evaluated one at a time from top to bottom. A shadow rule in a policy will never be matched because the network traffic matches a rule above the shadowed rule in the policy. If there is a shadowed rule that will never be hit, remove it, or edit the policy to make the rule effective.

Evaluate Policy Hit Rates

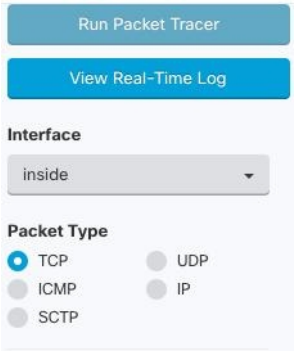
Determine if the rules in your policies are actually evaluating network traffic. CDO gathers hit rate data on the rules in your policies every hour. The longer your devices are managed by CDO the more meaningful the hit rate data on a particular rule is. Filter ASA access policies by hit count over the time period you're interested in to see if it is getting hit. If it is not, consider rewriting the policy or deleting it.



Troubleshoot Policies

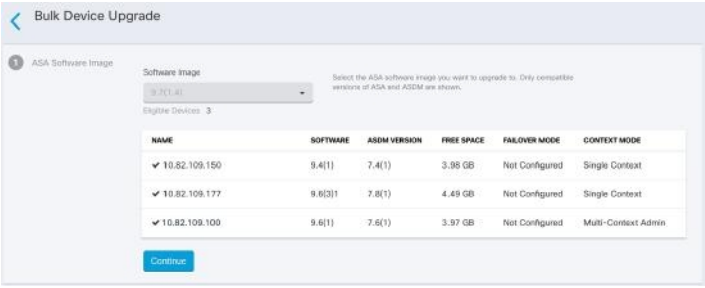
You can use the ASA Packet Tracer to test the path of a synthetic packet through a policy and determine if a rule is inadvertently blocking or allowing access.

Managing ASA with Cisco Defense Orchestrator



Upgrade ASA and ASDM

Next, upgrade to the newest version of ASA and ASDM. Customers have reported time-savings of 75%-90% when upgrading their ASAs using CDO.



CDO provides a wizard that allows you to upgrade the ASA and ASDM images installed on an individual ASA or on multiple ASAs in single-context or multi-context mode. CDO maintains a database of ASA and ASDM images.

CDO performs the necessary upgrade compatibility checks behind the scenes. The wizard guides you through the process of choosing compatible ASA and ASDM images, installing them, and rebooting the device to complete the upgrade. CDO secures the upgrade process by validating that the images you chose on CDO are the ones copied to, and installed on, your ASA.

CDO periodically reviews its database and adds the newest ASA and ASDM images to it. CDO only supports generally available (GA) images and does not add custom images to its database. If you do not see a specific GA image in the list, please contact Cisco TAC from the **Contact Support** page. We will process your request using the established support ticket SLAs and upload the missing GA image.

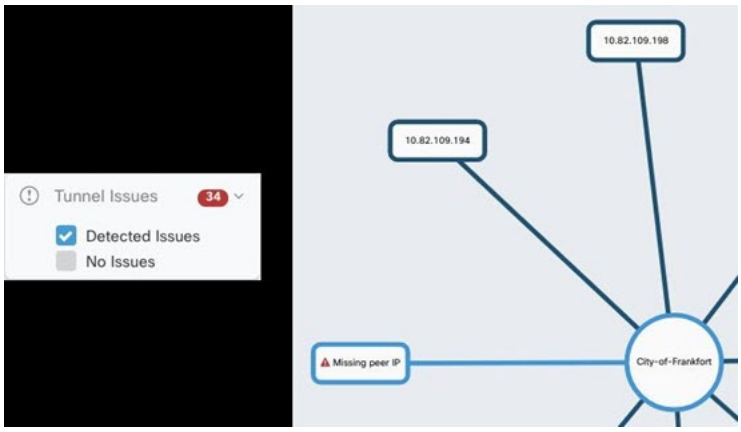
Review Upgrade ASA and ASDM Images on a Single ASA, on page 138 and then continue with Upgrade Multiple ASAs with Images from your own Repository, on page 137 to learn more about upgrading your ASAs.

Monitor and Manage VPN Connections

Review Site-to-Site VPN Issues

CDO reports VPN issues present on ASA devices in your network. You can look at your environment two ways, as a table showing a listing of VPN peers or a map showing your VPN connections in a hub and spoke topology. Use the filter sidebar to search of VPN tunnels that need your attention.

Managing ASA with Cisco Defense Orchestrator



Use CDO to evaluate your VPN tunnels:

- Check Site-to-Site VPN Tunnel Connectivity
- 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

Onboard Unmanaged Site-to-Site VPN Peers

CDO also identifies unmanaged VPN peers. Once you identify those device use Onboard an Unmanaged Site-to-Site VPN Peer, on page 274 to onboard the device and manage it with CDO as well.

ASA Remote Access VPN Support

CDO allows creating remote access virtual private network (RA VPN) configurations to allow users to securely access enterprise resources when connecting through the ASA. When your ASAs are onboarded to CDO, CDO recognizes any RA VPN settings that have already been configured using ASDM or Cisco Security Manager (CSM) so that you can manage them with CDO.

AnyConnect is the only client that is supported on endpoint devices for RA VPN connectivity.

CDO supports the following aspects of RA VPN functionality on ASA devices:

- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple ASA devices

See Configure Remote Access Virtual Private Network for ASA, on page 277 for more information.

Monitor Device Configuration Synchronization

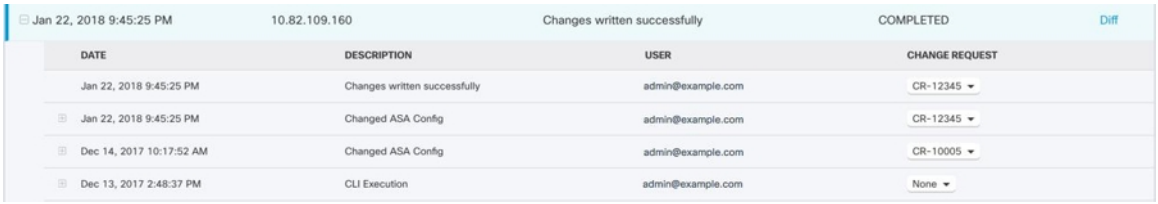
CDO periodically compares the device configuration it has stored in its database with the one installed on the ASA. The ASA you onboarded to CDO can still be onboarded ASA can still be managed by the device's Adaptive Security Device Manager (ASDM), so CDO makes sure that the configuration it has is the same as

the configuration on the device and alerts you to differences. See Conflict Detection, on page 243 for more information about the Synced, Not Synced or Conflict Detected device states.

Keep Track of Changes in the Change Log

The changes you make to your device's configurations are recorded in the Manage Change Logs in CDO, on page 321. The change log displays information like changes deployed from CDO to your device, changes imported from your device to CDO, what the change was along with the ability to see a "diff" of that change, when it happened, and who did it.

You can also Change Request Management, that uses your company's tracking number, to the changes you make. In the change log, you can filter the list of changes by that custom label, a date range, by a specific user, or by change type to find what you're looking for.



Restore a Previous Configuration

If you make changes to an ASA that you want to "undo," you can use CDO to restore the device to a previous configuration. See Restore an ASA Configuration, on page 227 for more information.

Managing Devices Using a Command Line Interface and Command Macros

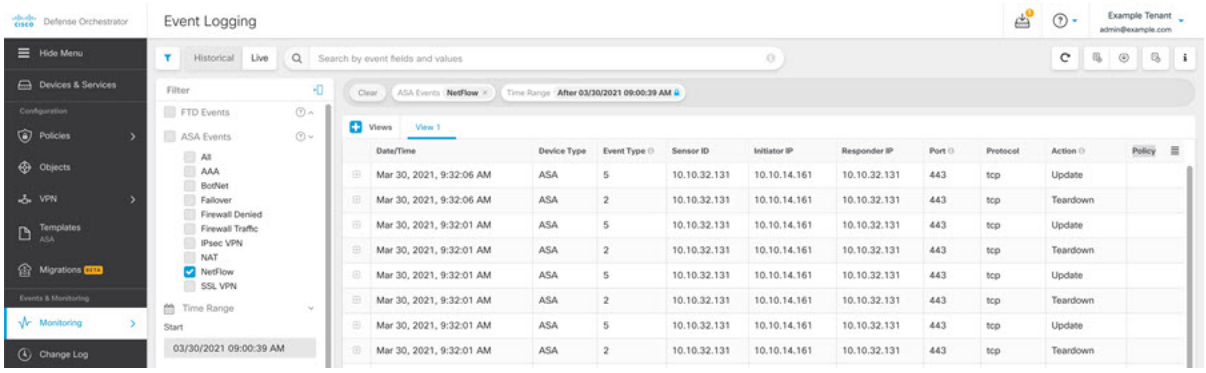
CDO is a web-based management product that provides you with both a graphic user interface (GUI) and a CDO Command Line Interface (CLI) to manage your devices one at a time or many at once.

ASA CLI users will appreciate the extra capabilities of our CLI tool. Here are some of the reasons to use CDO's CLI tool rather than connecting to the device with an SSH session:

- CDO knows what user mode is needed for a command. You do not need to elevate or lower your permission level to execute a command, nor do you need to enter the specific command context to execute a command.
- CDO retains command history, so you can easily re-run a command by picking it from a list.
- CLI actions are logged in the change log, so you can read what command was sent and what action was taken.
- Commands can be run in bulk mode, allowing you to deploy objects or policies to multiple devices simultaneously.
- CDO supplies CLI macros . CLI macros are stored ready-to-use commands you can run as they are, or "fill-in-the-blank" CLI commands you can complete and run. You can run these commands on one device or send the command to multiple ASAs at the same time.
- CLI provides you with the complete ASA configuration file. You can view it or, if you are an advanced user, edit it directly and save your changes rather than issuing CLI commands to change it.

Cisco Security Analytics and Logging

With additional licensing, Cisco Security Analytics and Logging, on page 335 allows you to direct syslog events and Netflow Secure Event Logging (NSEL) events from your ASA to a Secure Event Connectors, on page 370 (SEC), which then forwards them to the Cisco cloud. Once in the cloud, you can view those events in CDO's Event Logging page. There you can filter and review the events to gain a clear understanding of what security rules are triggering in your network.



In addition to monitoring events, you can launch the Secure Cloud Analytics portal from the CDO to perform behavioral analysis on the events that were logged.

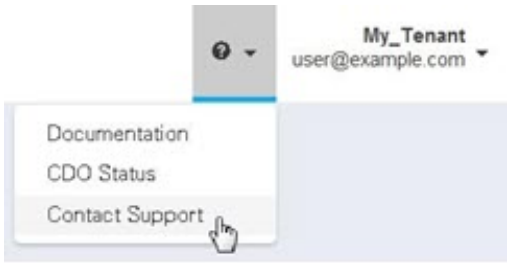
See Implementing Secure Logging Analytics (SaaS) for ASA Devices, on page 345 for a complete explanation of how to implement Cisco Security Analytics and Logging.

What to do Next

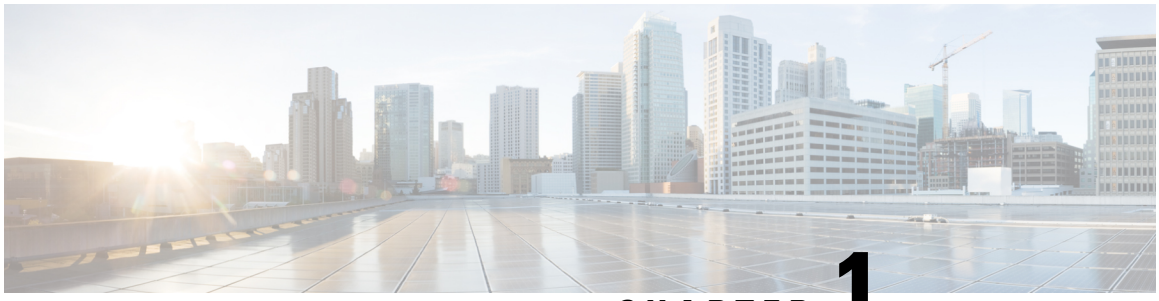
Now you can begin onboarding your ASA s and orchestrating your policies.

If You Need Help

You can Contact CDO Support, or read our product documentation by clicking on our support menu in the CDO GUI.



Managing ASA with Cisco Defense Orchestrator



CHAPTER 1

Basics of CDO

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

Create a CDO Tenant

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

Procedure

1. Go to https://www.defenseorchestrator.com/provision.
2. Select the region where you want to provision your CDO 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 you are prompted for, and click **Sign up**.

      Clicking on **Sign up** triggers a mail to the e-mail ID you just provided, with a link to activate your account.

   b. Click **Activate account** both on the mail and the **Security Cloud Sign On** page.

   c. 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 CDO tenant is created in the region you have chosen; you will also receive an e-mail about your CDO tenant being created, with the details. If you are associated with multiple CDO 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 CDO tenant for the first time, you get logged into your tenant directly.

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

   For information about managing a CDO tenant and various tenant settings, see Tenant Management.

Upgrade your CDO tenant to full version

If you are using a free trial version of CDO, you will keep seeing the **You are in a free trial of** CDO banner, with the number of days left in the trial period. You can choose to upgrade your CDO 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 CDO.

Request CDO trial period extension

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

Sign in to CDO

To log in to Cisco Defense Orchestrator (CDO), a customer needs an account with a SAML 2.0-compliant identity provider (IdP), a multi-factor authentication provider, and Manage Users in CDO.

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 CDO user record primarily contains the username, the CDO tenant with which they are associated, and the user's role. When a user logs in, CDO tries to map the IdP's user ID to an existing user record on a tenant in CDO. The user is logged in to that tenant when CDO finds a match.

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 multi-factor authentication. Customers can Integrate Your SAML Single Sign-On with if they choose.

To log into CDO, 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 CDO record.

On October 14, 2019, CDO 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 CDO 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 CDO, this transition did affect you.

If your CDO tenant was created on or after October 14, 2019, see Initial Login to Your New CDO Tenant, on page 3.

If your CDO tenant existed before October 14, 2019, see Migrate to Cisco Security Cloud Sign On Identity Provider, on page 4.

Initial Login to Your New CDO 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.

Cisco Defense Orchestrator (CDO) 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 CDO tenant using https://www.defenseorchestrator.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 CDO. 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 CDO tenant existed before October 14, 2019**, use Migrate to Cisco Security Cloud Sign On Identity Provider, on page 4 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 67. It is a four-step process. You need to complete all four steps.

Signing in to CDO in Different Regions

These are the URLs you use to sign in to Cisco Defense Orchestrator in different AWS regions:

Table 1: CDO URLs in Different Regions

Region	Cisco Defense Orchestrator URL
Asia-Pacific and Japan (APJ)	https://www.apj.cdo.cisco.com/
Australia (AUS)	https://aus.cdo.cisco.com
Europe, the Middle East, and Africa (EMEA)	https://defenseorchestrator.eu/
India (IN)	https://in.cdo.cisco.com
United States (US)	https://defenseorchestrator.com

Troubleshooting Login Failures

Login Fails Because You are Inadvertently Logging in to the Wrong CDO Region

Make sure you are logging into the appropriate CDO 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 CDO in Different Regions, on page 4 for information about which region you shoud sign into.

Migrate to Cisco Security Cloud Sign On Identity Provider

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

CDO 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 CDO. 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 CDO 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 CDO, this transition does apply to you.
- **If your CDO tenant was created on or after October 14, 2019**, see Initial Login to Your New CDO Tenant, on page 3 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 CDO Fails Because of Incorrect Username or Password

Solution If you try to log in to CDO 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 67.

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

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your CDO tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between CDO 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 CDO tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Defense Orchestrator APJ

- **Solution** Cisco Defense Orchestrator Australia
- **Solution** Cisco Defense Orchestrator EU
- **Solution** Cisco Defense Orchestrator India
- **Solution** Cisco Defense Orchestrator US

- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Launch a CDO Tenant

Step 1 Click the appropriate CDO 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 CDO 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 CDO or request a trial tenant.

The **Portals** view retrieves and displays consolidated information from multiple tenants. See Manage Multi-Tenant Portal, on page 56 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 CDO, and change the roles of other users to "Admin."

About CDO Licenses

CDO requires a base subscription for tenant entitlement and device licenses for managing devices. You can buy one or more CDO 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 CDO tenant, and for every device you choose to manage using CDO, you need separate device licenses.

For the purposes of planning your deployment, note that each CDO 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 Cisco Defense Orchestrator, you need to purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Cisco Defense Orchestrator subscriptions are term-based:

- **Base** - Offers subscriptions for one, three, and five years, and provides entitlement to access the CDO 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 CDO for three years, if you purchase a three-year software subscription to the Cisco Firepower 1010 device.

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

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

Note You cannot manage CDO licensing through the Cisco smart licensing portal.

Software Subscription Support

The CDO 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 CDO solution support based on your requirement.

Cisco Defense Orchestrator Evaluation License

You can request for a 30-day Cisco Defense Orchestrator trial from your SecureX account. See Request a CDO 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 CDO; the base subscription for a CDO 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 CDO tenant, see Request a Cloud-delivered Firewall Management Center for your CDO 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 Defense Orchestrator* for information.

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

The SDCmonitors CDO 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 CDO, sends messages to CDO on behalf of the managed devices, and returns replies from the managed devices to CDO.

The SDC uses secure communication messages signed and encrypted using AES-128-GCM over HTTPS (TLS 1.2) to communicate with CDO. 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 CDO service has access to the credentials. See Connect CDO to your Managed

Devices, on page 9 for information explaining how to allow communication between between an SDC and CDO.

The SDC may be installed on an appliance, as a virtual machine on a hypervisor, or in a cloud environment like AWS or Azure. You can install an SDC by using a combined virtual machine and SDC image provided by CDO, or you can create your own virtual machine and install the SDC on it. The SDC virtual appliance includes a CentOS or Ubuntu operating system and runs within a Docker container.

Each CDO 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 CDO 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 CDO tenant. Without multiple SDCs, you would need to manage the devices in those isolated network segments with different CDO tenants.

The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC. 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 CDO. Each additional SDC is numbered in order. See Deploy a Secure Device Connector Using CDO's VM Image, on page 11 and Deploy a Secure Device Connector On Your VM, on page 15

Related Information:

- Connect CDO to your Managed Devices
- Update your Secure Device Connector, on page 28
- Remove a Secure Device Connector, on page 27

Connect CDO to your Managed Devices

CDO 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 CDO 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 CDO to communicate with your devices.

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

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

- An ASA device that is not accessible from the cloud.

All other devices and services do not require an on-premise SDC. CDO 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 CDO Through the Cloud Connector

When connecting CDO 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 CDO at https://www.apj.cdo.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 CDO at https://aus.cdo.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 CDO at https://defenseorchestrator.eu/, 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 CDO at https://in.cdo.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 CDO at https://defenseorchestrator.com, allow inbound access from the following IP addresses:

- 52.34.234.2
- 52.36.70.147

Connecting CDO to SDC

When connecting CDO to your device through an SDC, the devices you want CDO to manage must allow full inbound access 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.

Special Consideration for Connecting an ASA to an SDC

Specifically, for ASA the SDC uses the same secure communications channel used by ASDM.

If the ASA under management is also configured to accept AnyConnect VPN Client connections, the ASDM HTTP server port must be changed to a value of 1024 or higher. Note that this port number will be the same port number used when onboarding the ASA device into CDO.

Example ASA Commands

The following examples assume that the ASA outside interface is named 'outside' and an AnyConnect client is configured on the ASA so the ASDM HTTP server is listening on port 8443.

To enable the outside interface, enter these commands:

Asia-Pacific-Japan Region:

- http 54.199.195.111 255.255.255.255 outside
- http 52.199.243.0 255.255.255.255 outside

Australia Region

- http 13.55.73.159 255.255.255.255 outside
- http 13.238.226.118 255.255.255.255 outside

EMEA Region

- http 35.157.12.126 255.255.255.255 outside
- http 35.157.12.15 255.255.255.255 outside

India Region

- http 35.154.115.175 255.255.255.255 outside
- http 13.201.213.99 255.255.255.255 outside

United States Region

- http 52.34.234.2 255.255.255.255 outside
- http 52.36.70.147 255.255.255.255 outside

To enable the ASDM HTTP server port, in the case where AnyConnect VPN Client is in use, enter this command:

http server enable 8443

Deploy a Secure Device Connector Using CDO's VM Image

When using device credentials to connect CDO to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between CDO 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 CDO using an SDC.

The SDC monitors CDO 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 CDO, sends messages to CDO on behalf of the managed devices, and returns replies from the managed devices to CDO.

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 CDO Tenant, on page 29 for more information.

This procedure describes how to install an SDC in your network, using CDO'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 15.

Before you begin

Review these prerequisites before you deploy the SDC:

- CDO 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 CDO.
- 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 CDO must also allow inbound traffic from this port.
- Review Connect CDO to your Managed Devices to ensure proper network access.
- CDO supports installing its SDC VM OVF image using the vSphere web client or the ESXi web client.
- CDO 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 CDO).

  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.

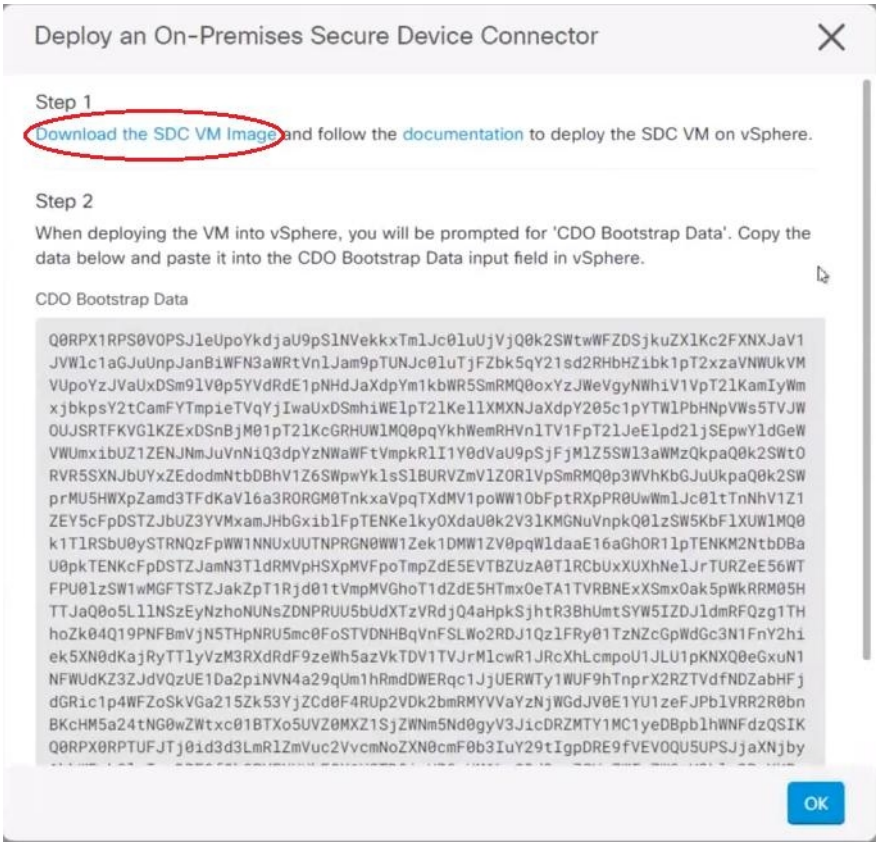
- The FQDN or IP address of your time server.
- The SDC virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

Step 1 Log on to the CDO Tenant you are creating the SDC for.

Step 2 From the CDO menu, choose **Tools & Services** > **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 CDO user. Enter your password for the user

Step 15 When prompted with **Please choose the CDO domain you connect to**, enter your Cisco Defense Orchestrator 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
```

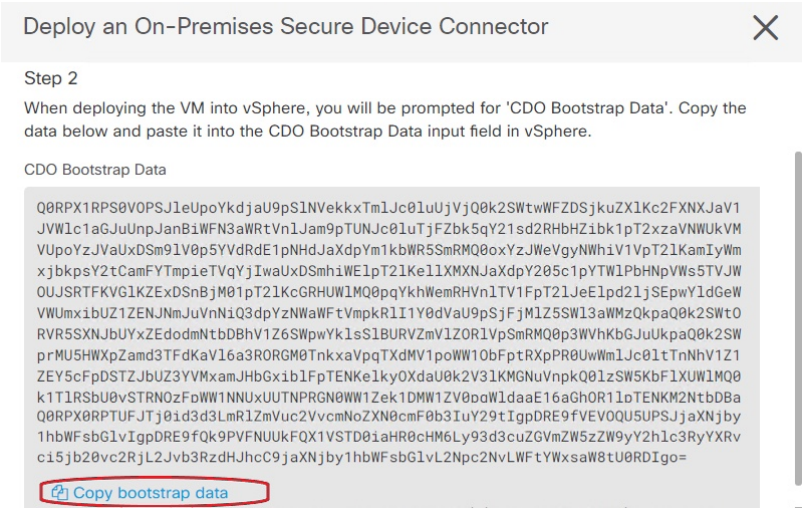
Step 23 When prompted with **[sudo] password**, enter the password you created in Step 14.

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

a. Log into CDO.

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 CDO 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 CDO 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 CDO using device credentials.

The SDC monitors CDO 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 CDO, sends messages to CDO on behalf of the managed devices, and returns replies from the managed devices to CDO.

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 CDO Tenant, on page 29 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 CDO's SDC OVA image and install it. See Deploy a Secure Device Connector Using CDO's VM Image, on page 11 for those instructions.

Before you begin

- CDO 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 CDO.
- Devices that reach CDO through the SDC must allow inbound access from the SDC on port 443.
- Review Connect CDO 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 CDO).

  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.

Step 1 Log on to the CDO tenant you are creating the SDC for.

Step 2 In the left pane, choose **Tools & Services** > **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 CDO.

```
[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 CDO.

What to do next

-
- Return to Install a Secure Event Connector on an SDC Virtual Machine, on page 371 if you are installing a Secure Event Connector.
- Return to Installing an SEC Using a CDO 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 CDO 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 CDO 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 CDO using device credentials.

The SDC monitors CDO 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 CDO, sends messages to CDO on behalf of the managed devices, and returns replies from the managed devices to CDO.

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 CDO 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

- CDO 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 CDO 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.

Step 1 Log on to the CDO tenant you are creating the SDC for.

Step 2 Choose **Tools & Services** > **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 CDO 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 CDO
Event Connectors panel.
```

The Secure Device Connector must now show "Active" in CDO.

What to do next

-
- Go to Deploy Secure Event Connector on Ubuntu Virtual Machine, on page 379 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 CDO SDC Terraform module for vSphere in conjunction with the CDO 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

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

Step 2 Configure the CDO Terraform provider in your Terraform repository by following the instructions in CDO 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 CDO Terraform provider. See the Terraform registry for CDO-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 CDO 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 CDO_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 CDO 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 CDO 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:

- CDO 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) andCDO.
- Review Connect CDO 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 CDO 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.

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 CDO 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 CDO. 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.

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 CDO after changing the SDC's IP address.

Step 1 Create an SSH connection to your SDC or open your virtual machine's console, and log in as the CDO 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 cdo:
```

Step 5 Type `n` at the prompt for resetting the root and CDO 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 CDO user interface. To do that, open the CDO application and navigate to **Tools & Services** > **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 15 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:

Step 1 Remove any devices connected to the SDC you want to delete. You can do this one of two ways:

- Move some devices to different SDCs or off of an SDC entirely. See below for more information:
- Remove from CDO any devices connected to the SDC you want to delete.
  a. See CDO 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, choose **Tools & Services** > **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 CDO 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

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

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab and then 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 CDO 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

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 CDO interface including the Secure Device Connectors filter of the **Inventory** pane.

Specify a Default Secure Device Connector

Many devices managed by CDO, though not all, connect to CDO through a SDC. When you onboard devices that connect to CDO through an SDC, they are associated with the default SDC for your tenant unless you specify otherwise during onboarding.

You can specify which SDC is selected by default on the Secure Connectors page:

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

Step 2 Select the SDC that you want to be the default.

Step 3 In the Actions pane, click **Make Default**. If you don't see the Make Default action, then the SDC already is the default SDC.

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.

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 CDO 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 CDO tenant. Without multiple SDCs, you would need to manage the devices in isolated network segments with different CDO tenants.

The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC. Deploy a Secure Device Connector Using CDO'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.

CDO Devices that Use the Same SDC

Follow this procedure to identify all the devices that connect to CDO using the same SDC:

Step 1 In the navigation bar, click **Inventory**.

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 CDO.

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 CDO 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 CDO.

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.

==========

*** when ***

Open Source Initiative OSI - The MIT License

http://www.opensource.org/licenses/mit-license.php

Copyright (c) 2011 Brian Cavalier

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

Devices, Software, and Hardware Supported by CDO

CDO is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms. CDO 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 CDO supports. It does not point out software and devices that CDO 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. CDO 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, Cisco Defense Orchestrator, 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

CDO 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. CDO supports managing layer 3 network rules on Meraki MX devices. When you onboard a Meraki device to CDO, it communicates with the Meraki dashboard to manage that device. CDO securely transfers configuration requests to the Meraki dashboard, which then applies the new configuration to the device. Key features of CDO'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

CDO 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

CDO 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.

ASA Support Specifics

CDO can manage all platforms running ASA 8.4 and later (see ASA and ASDM Compatibility Per Model), including ASAv instances, except for the ASA Services Module (ASASM), which is not supported by CDO.

CDO can onboard an ASA running ASA 8.3 but cannot deploy changes to it or manage it in any other way. Support is "read-only."

There may be a CDO feature that does not support all versions of ASA, such as Prerequisites for ASA and ASDM Upgrade in CDO" from pre-9.12 versions. In those cases, the CDO documentation will list any version exceptions with the prerequisites for that feature.

CDO does not manage the ASA FirePOWER module, which runs a different operating system from ASA. You must manage an ASA FirePOWER module separately with Firepower Management Center or ASDM.

Note EOL code and hardware may continue work with CDO, but we cannot assure all functionality of CDO with respect to EOL code and hardware, as it is not part of our testing. CDO makes no guarantees nor assurances of correct operation with EOL software and hardware. An example of this would be the EOL ASA versions 8.x, 9.1, and 9.2 do not support TLS 1.2 on the management plane and would be considered an insecure way to manage ASA software.

Please defer to the version download page for Cisco "suggested release" or "gold star" versions.

For a full discussion of ASA, ASDM, and hardware compatiblity, see the Cisco Secure Firewall ASA Compatibility guide.

Cloud Device Support Specifics

The following table describes software and device type support for cloud-based devices. Read the affiliated links for more information about onboarding and feature functionality for the device types in the table below:

Devices Types	Notes
Google Cloud Platform	Google Cloud Platform (GCP) receives any updates through the GCP console. See Google Cloud documentation for more information on the platform and available services. See
Microsoft Azure	Azure receives any updates through the Azure console. See Azure documentation for more information on the platform and available services.

Browsers Supported in CDO

CDO supports the latest version of these browsers:

- Google Chrome
- Mozilla Firefox

CDO Platform Maintenance Schedule

CDO 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 CDO continue to enforce their security policies.

Note

- We advise against using CDO to deploy configuration changes on the devices it manages during maintenance periods.
- If there is any issue that stops CDO 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 CDO updates the cloud-delivered Firewall Management Center environment. Super Admin and Admin users of the tenant are notified by email. CDO 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 CDO 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 CDO Tenant

CDO 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

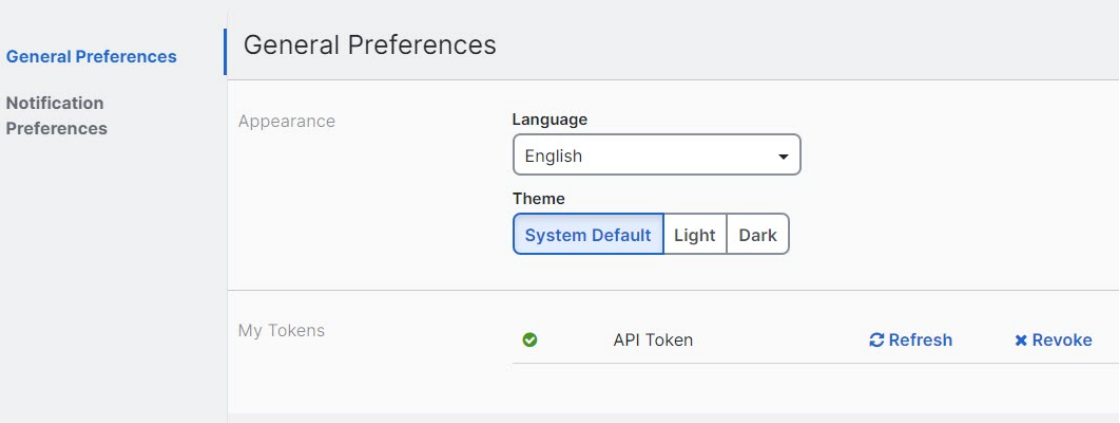
See the following topics regarding general CDO Settings:

- General Preferences, on page 43
- For **My Tokens**, see API Tokens, on page 53

- For **Tenant Settings**, see:
  - Enable Change Request Tracking, on page 44
  - Prevent Cisco Support from Viewing your Tenant, on page 44
  - Enable the Option to Auto-accept Device Changes, on page 44
  - Enable the Option to Schedule Automatic Deployments, on page 45
  - Default Conflict Detection Interval, on page 44
  - Web Analytics, on page 45
  - Tenant ID, on page 46
  - Tenant Name, on page 46

General Preferences

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



Change the CDO Web Interface Appearance

You can change the way the web interface appears.

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:

Step 1 From the CDO menu bar, select **Settings** > **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 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:

Step 1 From the CDO menu bar, select **Settings** > **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 Cisco Defense Orchestrator 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:

Step 1 In the left pane, click **Settings** > **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 CDO 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:

Step 1 From the CDO menu bar, select **Settings** > **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 CDO 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 CDO 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:

Step 1 From the CDO menu bar, select **Settings** > **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:

Step 1 From the CDO menu bar, select **Settings** > **General Settings**.

Step 2 In the Tenant Settings area, click the slider 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.

Step 1 From the CDO menu bar, select **Settings** > **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**.

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).

View CDO 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 CDO. 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 CDO.

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 CDO 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 CDO across all pages. From this page you can configure the following "**Notify Me in CDO 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 FTD to cloud** - This action is applicable when changing the FTD

device manager from FMC to CDO.

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 CDO 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 CDO 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 CDO for more information.

Email Subscribers

Add or modify the emails that receive alerts from your CDO tenant. See Enable Email Subscribers, on page 49 for more information.

Service Integrations

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

Enable Email Subscribers

An email notification from CDO 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 CDO and examining the Manage Change Logs in CDO of the affected devices.

Warning Be sure to enter the correct email if you are adding a mailer. CDO 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.

Step 1 Log into CDO and navigate to **Settings** > **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.

Step 1 Log into CDO and navigate to **Settings** > **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.

Step 1 Log into CDO and navigate to **Settings** > **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 CDO Notifications

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

CDO 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

CDO 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 CDO account and tenant.

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

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 aWebex 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 CDO.

Step 7 From the navigation bar to the left, click **Settings** > **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 CDO 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

CDO 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:

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 CDO 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 CDO.

Step 9 From the navigation bar to the left, click **Settings** > **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 CDO 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

CDO does not format messages for custom integration. If you opt to integrate a custom service or application, CDO 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:

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

Step 2 Log into CDO.

Step 3 From the navigation bar to the left, click **Settings** > **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 CDO 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

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

If, however, customers want to integrate their own SAML single sign-on IdP solution with CDO, 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 CDO, 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 CDO, open a How CDO Customers Open a Support Ticket with TAC and provide the metadata.xml file.

API Tokens

Developers use CDO API tokens when making CDO 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 CDO. 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 CDO 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 CDO 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

Step 1 From the navigation bar to the left, click **Settings** > **General Settings**.
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.

Step 1 From the navigation bar to the left, click **Settings** > **General Settings**.
Step 2 In My Tokens, click **Renew**. CDO 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

Step 1 From navigation bar to the left, click **Settings** > **General Settings**.
Step 2 In My Tokens, click **Revoke**. CDO revokes the token.

Relationship Between the Identity Provider Accounts and CDO User Records

To log in to CDO, a customer needs an account with a SAML 2.0-compliant identity provider (IdP), a multi-factor authentication provider, and a user record in CDO. 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 CDO user record primarily contains the username, the CDO tenant with which they are associated, and the user's role. When a user logs in, CDO tries to map the IdP's user ID to an existing user record on a tenant in CDO. When CDO 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 if they choose.

Login Workflow

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

Step 1 The user requests access to CDO 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 CDO.

Step 3 CDO 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 CDO, CDO 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, CDO 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 CDO does not have a mapping for the authenticated user to a user record on a tenant, CDO displays a landing page giving users the opportunity to learn more about CDO or request a free trial.

Creating a user record in CDO does not create an account in the IdP and creating an account in the IdP does not create a user record in CDO.

Similarly, deleting an account on the IdP does not mean you have deleted the user record from CDO; although, without the IdP account, there is no way to authenticate a user to CDO. Deleting the CDO user record does not mean you have deleted the IdP account; although, without the CDO user record, there will be no way for an authenticated user to access a CDO tenant.

Implications of this Architecture

Customers Who Use Cisco Security Cloud Sign On

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

Should the Super Admin ever need to prevent a user from accessing CDO, they can simply delete the CDO 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 CDO 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 CDO 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 , they control both the identity provider accounts and the CDO tenants. These customers can create and manage identity provider accounts and user records in CDO.

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

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

Cisco Managed Service Providers

If Cisco Managed Service Providers (MSPs) use CDO'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 CDO 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 CDO
- User Roles in CDO

Manage Multi-Tenant Portal

CDO 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.

Note From the multi-tenant portal, you can add tenants across multiple regions and view devices those tenants manage. You cannot edit any tenants or configure any devices from the multi-tenant portal.

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 clearing cache and cookies from your web browser to avoid certain browser-related issues that may occur.

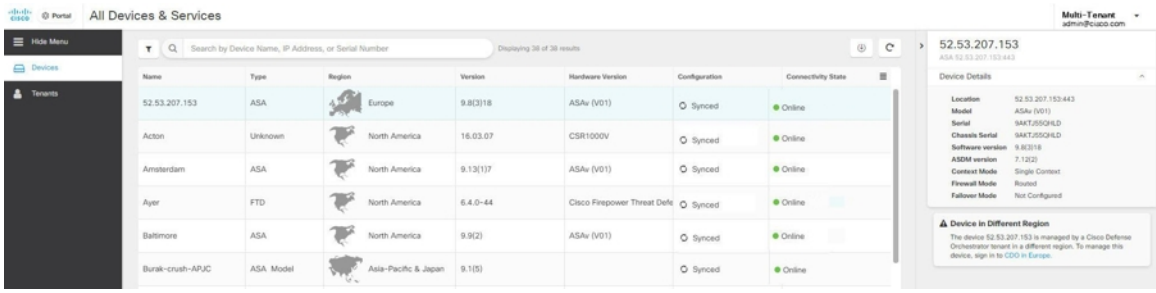
The Multi-Tenant Portal

The portal provides the following menus:

- **Devices**:

- Displays all the devices residing in the tenants added to the portal. Use the **Filter** and **Search** field to search devices that you want to view. You can click a device to view its status, the onboarding method, firewall mode, failover mode, software version, and many more.
- The interface provides a column picker that allows you to select or clear the device properties to view in the table. Except for 'AnyConnect Remote Access VPN', all the other device properties are selected by default. If you customize the table, CDO remembers your selection the next time you sign in to CDO.
- You can click on a device to see its details on the right.
- You can export the portal's information to a comma-separated value (.csv) file. This information helps you to analyze the devices or send it to someone who doesn't have access. Every time you export the data, CDO creates a new .csv file, where the file created has a date and time in its name.
- You can manage a device only from the CDO tenant that manages it. The multi-tenant portal provides the **Manage devices** link that directs you to the CDO tenant page. You'll see this link on the device 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'll not see the Manage Devices link. You can contact a super-admin in your organization for permission.

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



- **Tenants**:
  - Displays the tenants added to the portal.
  - It allows a Super Admin user to add tenants to the portal.
  - You can click to view the CDO tenant's main page.

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

- Create a CDO tenant
- Add an existing CDO 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 CDO.

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.

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

Step 2 Click **Generate API Token** and then copy it.

Step 3 Go to the portal and click the **Tenants** tab.

Step 4 Click add the tenant button on the right.

Step 5 Paste the token and click **Save**.

Delete a Tenant from a Multi-Tenant Portal

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

Cisco Defense Orchestrator 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. From the CDO dashboard, click **Settings** in the navigation bar to the left.
2. Click **General Settings**.

3. 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 CDO.

Switch Tenant

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

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.
- CDO 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 CDO 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 CDO

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

Unless your enterprise has its own IdP, Cisco Secure Sign-On is the identity provider for all CDO 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

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

Note To prevent Cisco support from accessing your tenant, enable **Prevent Cisco support from viewing this tenant** 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 CDO to your Active Directory (AD) groups instead of adding individual users to CDO 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 CDO.

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 CDO for more information.

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

Active Directory Groups Tab

In the left pane, choose **Settings** > **User Management** > **Active Directory Groups**. This page shows the Active Directory groups that are currently mapped to CDO. Most importantly, 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.

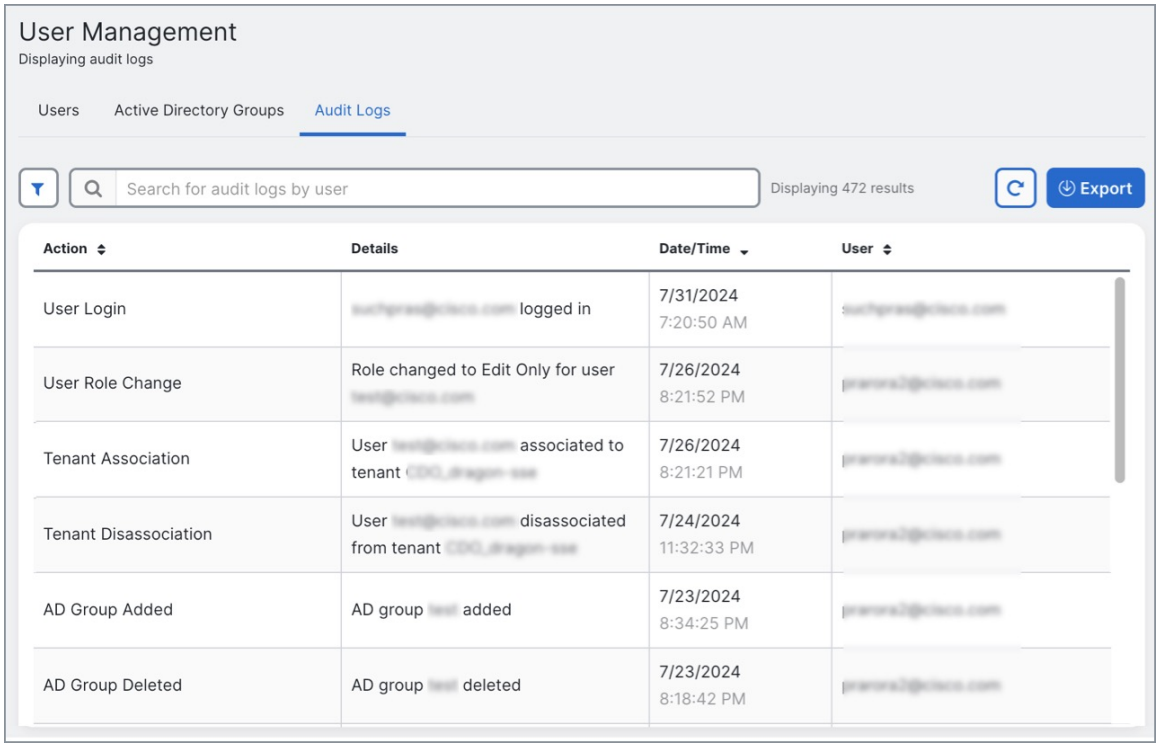
Audit Logs

Audit Logs in CDO 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.

1. In the left pane, click **Settings** > **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 1: Audit Logs



Multi-role Users

As an extension along the IAM capabilities in CDO, 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 CDO with different CDO 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 CDO 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 CDO 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 CDO, 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 CDO

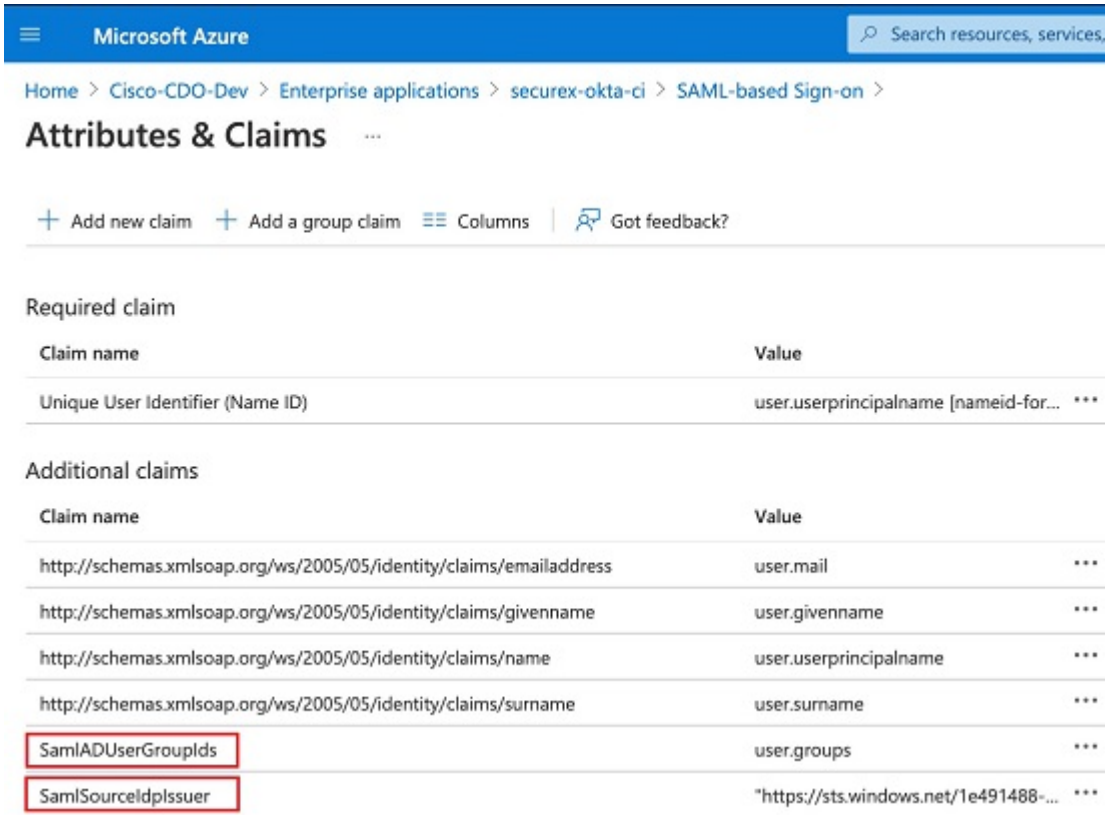
Before adding an Active Directory group mapping to CDO as a form of user management, you must have your Active Directory that is integrated with Security Cloud Sign On. If your Active Directory Identity Provider (IdP) is not already integrated, see identity provider integration guide to integrate a custom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

- Your CDO 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 CDO tenant after your Active Directory integration is done. These values are case sensitive:

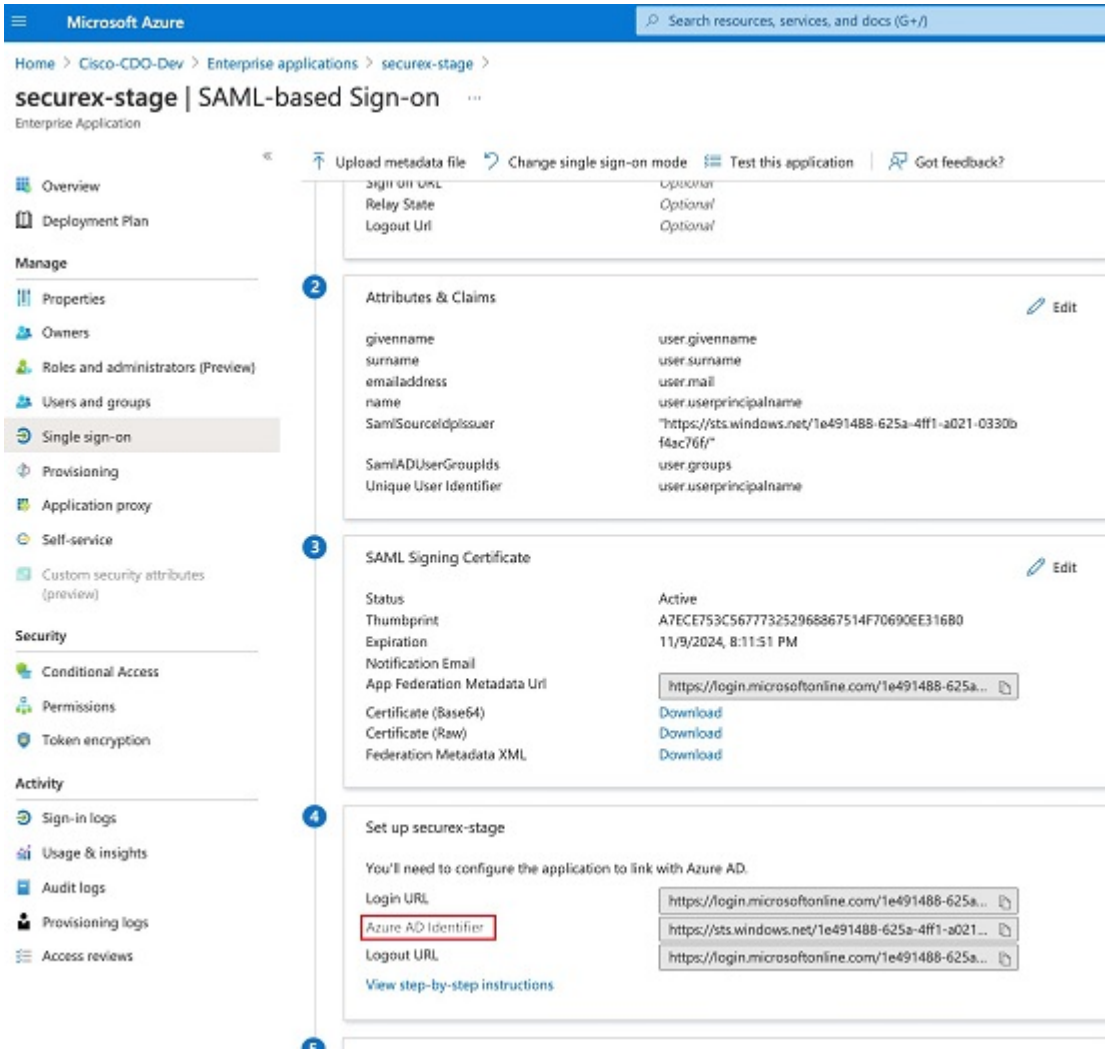
- **SamlADUserGroupIds** - This attribute describes all group associations that a user has on Active Directory. For example, in Azure select **+ Add a group claim** as seen in the screenshot below:

Figure 2: 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 3: 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.

Step 1 Log in to CDO.

Step 2 In the left pane, choose **Settings** > **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. CDO 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 CDO 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 CDO only allows you to modify how CDO limits the Active Directory group. You cannot edit the Active Directory group itself in CDO. You must use Active Directory to edit the list of users within an Active Directory group.

Step 1 Log in to CDO.

Step 2 In the left pane, choose **Settings** > **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. CDO 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

Step 1 Log in to CDO.

Step 2 In the left pane, choose **Settings** > **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 CDO User

These two tasks are necessary for creating a new CDO 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 CDO Username

After these tasks are done, then the user can The New User Opens CDO 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 CDO

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

CDO 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 CDO. 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 CDO tenant existed before October 14, 2019**, use Migrate to Cisco Security Cloud Sign On Identity Provider, on page 4 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.

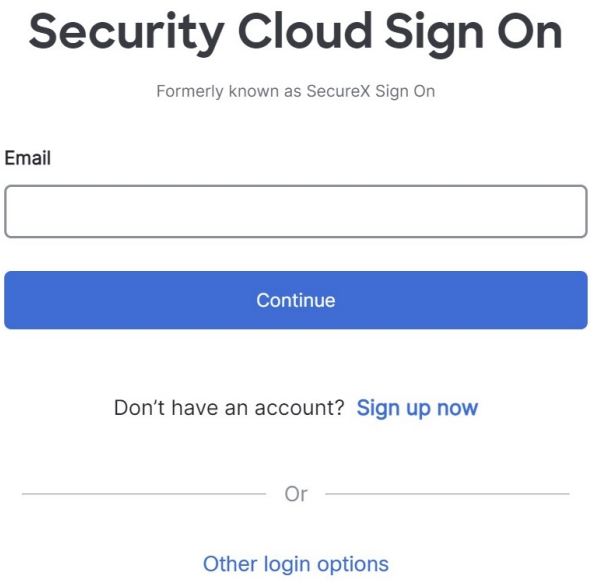
Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication

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

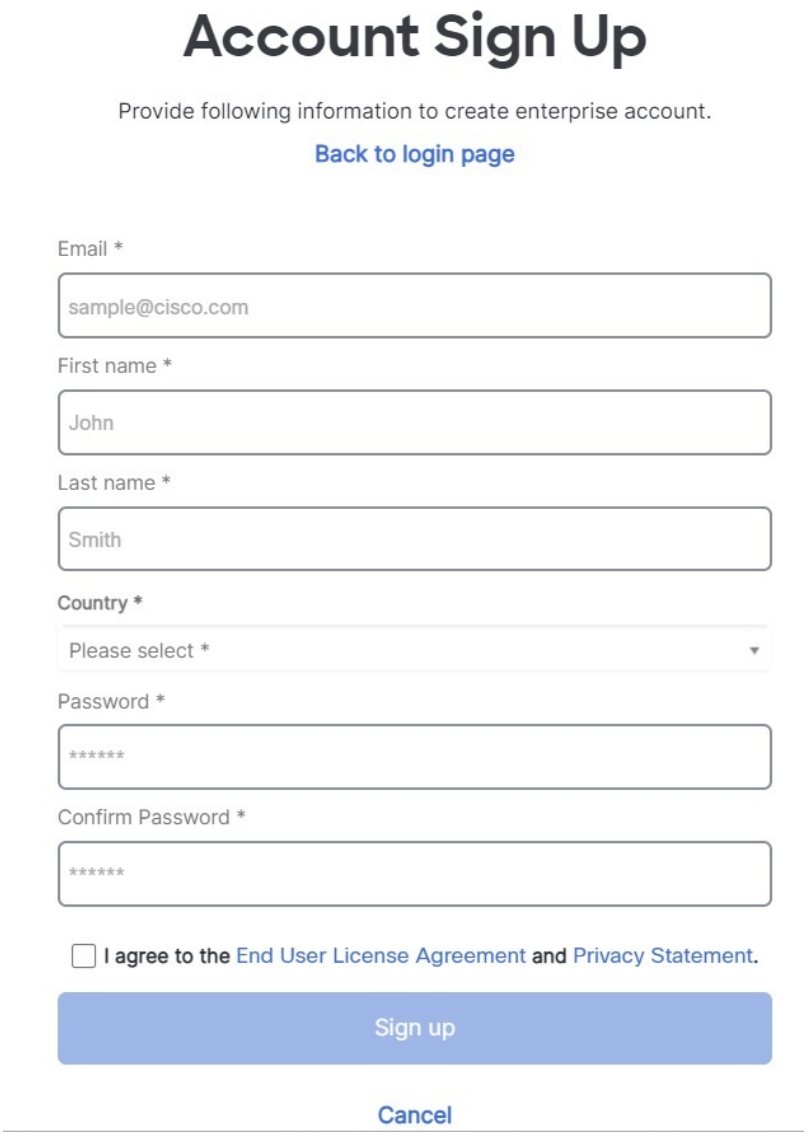
Step 1 **Sign Up for a New Cisco Security Cloud Sign On Account**.

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 CDO.
- **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 CDO Username

Only a CDO user with **Super Admin** privileges can create the CDO user record. The **Super Admin** must create the user record with the same email address that was specified in the **Create Your CDO Username** task above.

Use the following procedure to create a user record with an appropriate user role:

Step 1 Login to CDO.

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 CDO.

Step 6 Click **OK**.

The New User Opens CDO from the Cisco Secure Sign-On Dashboard

Step 1 Click the appropriate **CDO** tile on the Cisco Secure Sign-on dashboard. The **CDO** tile directs you to https://defenseorchestrator.com and the **CDO (EU)** tile directs you to https://defenseorchestrator.eu.

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 CDO 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 CDO 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 CDO

There are a variety of user roles in CDO: Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a CDO 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:

Read Only User. You cannot make configuration changes.

Users with the Read-Only role can do the following:

- View any page or any setting in CDO.
- 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 CDO 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 CDO 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 CDO 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 CDO.
- 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 CDO user records.
- Change user role.
- Attach or detach access rules to a policy.

Admin Role

Admin users have complete access to most aspects of CDO. Admin users can do the following:

- Create, read, update, and delete any object or policy in CDO and configure any setting.
- Onboard devices.
- View any page or any setting in CDO.
- 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 CDO user records.
- Change user role.

Super Admin Role

Super Admin users have complete access to all aspects of CDO. Super Admins can do the following:

- Change a user role.
- Create user records.

Note Though Super Admins can create a CDO 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 CDO Tenant, on page 3 for more information.

- Create, read, update, and delete any object or policy in CDO and configure any setting.
- Onboard devices.
- View any page or any setting in CDO.
- 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 CDO for more information.

You must be a Super Admin to change the user record. If your tenant has no Super Admins, contact How CDO Customers Open a Support Ticket with TAC.

Add a User Account to CDO

CDO users need a CDO record and a corresponding IdP account so they can be authenticated and access your CDO tenant. This procedure creates the user's CDO 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 CDO to perform this task.

Create a User Record

Use the following procedure to create a user record with an appropriate user role:

Step 1 Log in to CDO.

Step 2 From the CDO navigation bar, click **Settings** > **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 CDO from the drop-down menu.

Step 6 Click **v**.

Note Though Super Admins can create a CDO 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 CDO Tenant, on page 3 for more information.

Create API Only Users

Step 1 Log in to CDO.

Step 2 From the CDO navigation bar, click **Settings** > **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 CDO 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 CDO 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 CDO 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 CDO 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:

Step 1 Log in to CDO.

Step 2 From the CDO navigation bar, click **Settings** > **User Management**.

Step 3 Click the edit icon in the user's row.

Step 4 Select the user's new User Roles in CDO 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 CDO 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 CDO prevents the associated user from logging in to CDO 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 CDO 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 CDO to perform this task.

Delete a User Record

To delete the role defined in the user record, see the following procedure:

Step 1 Log in to CDO.

Step 2 From the CDO navigation bar, click **Settings** > **User Management**.

Step 3 Click the trash can icon in the row of the user you want to delete.

Step 4 Click **OK**.

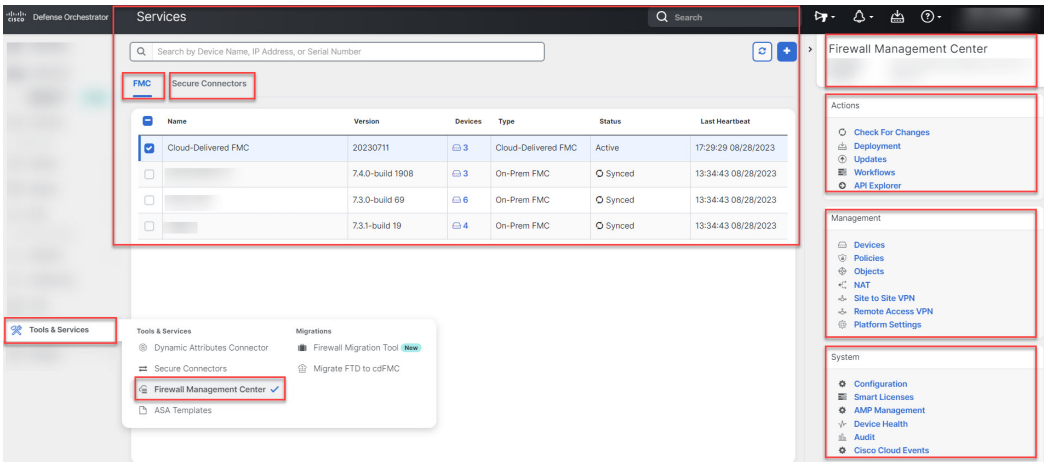
Step 5 Confirm that you want to remove the account from the tenant by clicking OK.

CDO Services Page

The **Services** page displays a list of services that CDO provides. Selecting the **FMC** tab lists the cloud-delivered Firewall Management Center that is linked to the CDO account and all the on-prem management centers onboarded to CDO. 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-prem 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-prem management center are filtered automatically and displayed. The **Services** page also allows you to select more than one on-prem management center at a time for you to perform actions on a group of management centers all at once. You cannot select any on-prem 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 **Tools & Services** > **Firewall Management Center**.



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 CDO 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 CDO 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 CDO 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 CDO 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 CDO 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 CDO 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 CDO that are generated from the security policies.

This feature is available for all CDO 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 CDO 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 CDO 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 CDO 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 Defense Orchestrator
- Onboard an On-Prem Firewall Management Center
- Request a cloud-delivered Firewall Management Center for your CDO tenant
- Secure Device Connector
- Secure Event Connectors

CDO Device and Service Management

CDO 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 CDO management.
- View the configuration state and connectivity state of managed devices and services.

- View onboarded devices and templates categorized in separate tabs. See CDO Inventory Information, on page 87.
- 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-prem 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 89.
- 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 CDO

When you onboard an device to Cisco Defense Orchestrator using an IP address, CDO 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 CDO to match the new address. Changing the device's IP address on CDO does not change device's configuration.

To change the IP address, CDO uses to communicate with a device, follow this procedure:

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

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 86

• Bulk Reconnect Devices to CDO, on page 86

Changing a Device's Name in CDO

All devices, models, templates, and services are given a name when they are onboarded or created in CDO. You can change that name without changing the configuration of the device itself.

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

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.

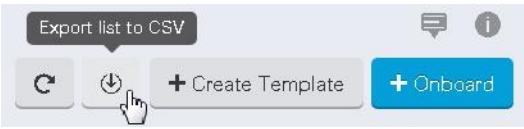
Step 1 In the left pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the 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:

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 appropriate device type tab.

You can use the Filters and Page Level Search functionalities to find the required device.

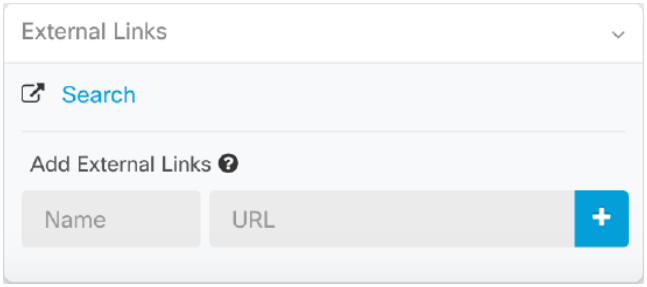
Step 4 Select the device you want so it is highlighted.

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 CDO. You could use this feature to create a convenient link to the local manager of one of your devices (Adaptive Security Device Manager (ASDM) for ASA). 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}
```

should reach the ASDM for your ASA .

Related Information:

- Write a Device Note, on page 87
- Export a List of Devices and Services, on page 82

Create an External Link from your Device

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 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 ASDM

Here is a convenient way to open the Adaptive Security Device Manager (ASDM) of your ASA , directly from CDO.

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 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 ASDM .

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

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 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

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 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

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 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 CDO

CDO allows an administrator to attempt to reconnect more than one managed device to CDO at the same time. When a device CDO manages is marked "unreachable," CDO 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 CDO's management of the device.

Note If you are reconnecting devices having new certificates, CDO 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, CDO prompts you to review and accept the certificate manually to continue to reconnect with it.

Step 1 In the navigation bar, click **Inventory**.

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 CDO 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 CDO, on page 330.

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 CDO tenant, you cannot migrate the devices from one CDO 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 CDO, while the Cisco Secure Client (formerly AnyConnect) is necessary for using virtual private network features on ASA, FDM-managed, and FTD devices from CDO.

CDO 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.

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 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.

CDO 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 CDO.
- The **Templates** shows all the template devices created from live devices or configuration files imported to CDO.

CDO 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:

Step 1 To add a label to a device, click **Inventory** in the navigation pane on the left. To add a label to an object, click **Objects** in the navigation pane on the left.

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 one or more devices or model in the generated table.

Step 5 In the **Add Groups and Labels** field on the right, specify a label for the device.

Step 6 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:

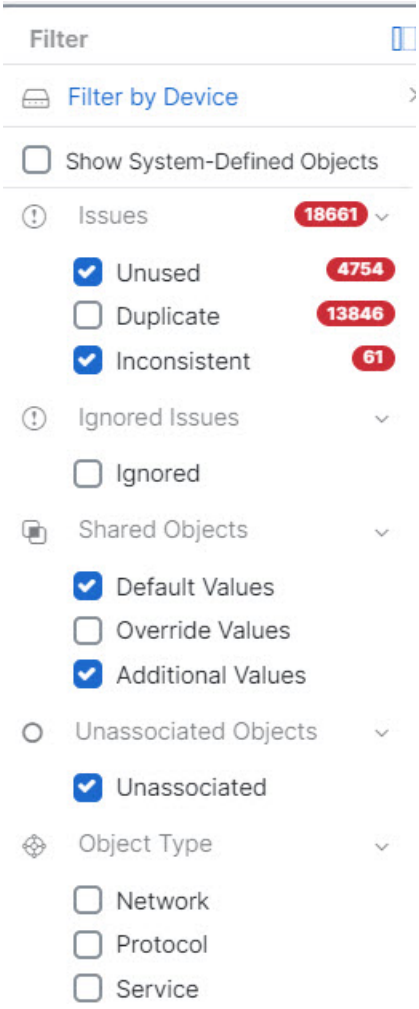
The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

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 CDO Search Functionality

The CDO 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.

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 CDO.

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 91.

- 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 CDO 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 CDO, 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

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

Step 2 In Global Search, click **Initiate Full Indexing** to trigger indexing.

Note Initiating full indexing clears existing indexing of the CDO tenant.

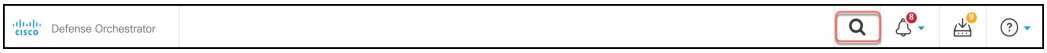
Step 3 Click **here** to view the global search workflow.

Perform a Global Search

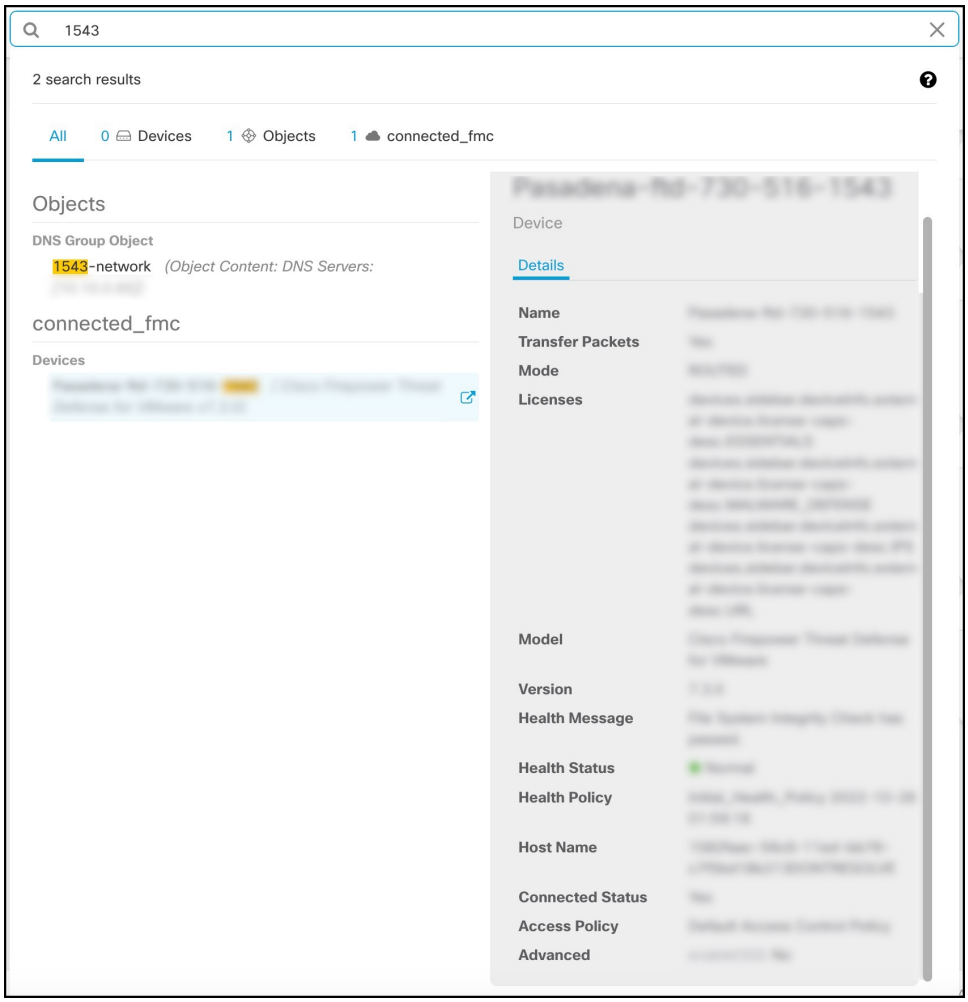
Step 1 Log into CDO.

Step 2 Click the search icon in the top-right corner of the CDO 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 CDO.

For information on cloud-delivered Firewall Management Center, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator.

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, CDO 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.

CDO 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, CDO 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, CDO does not do that anymore. You can use an unassociated object in a rule or a policy but there are no duplicate objects that CDO creates.

You can view the objects managed by CDO by navigating to the **Objects** menu or by viewing them in the details of a network policy.

CDO allows you to manage network and service objects across supported devices from one location. With CDO, 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 CDO.

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 242.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Cisco Defense Orchestrator, on page 496 for more information.

Object Types

The following table describes the objects that you can create for your devices and manage using CDO.

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: Adaptive Security Appliance (ASA) Object Types

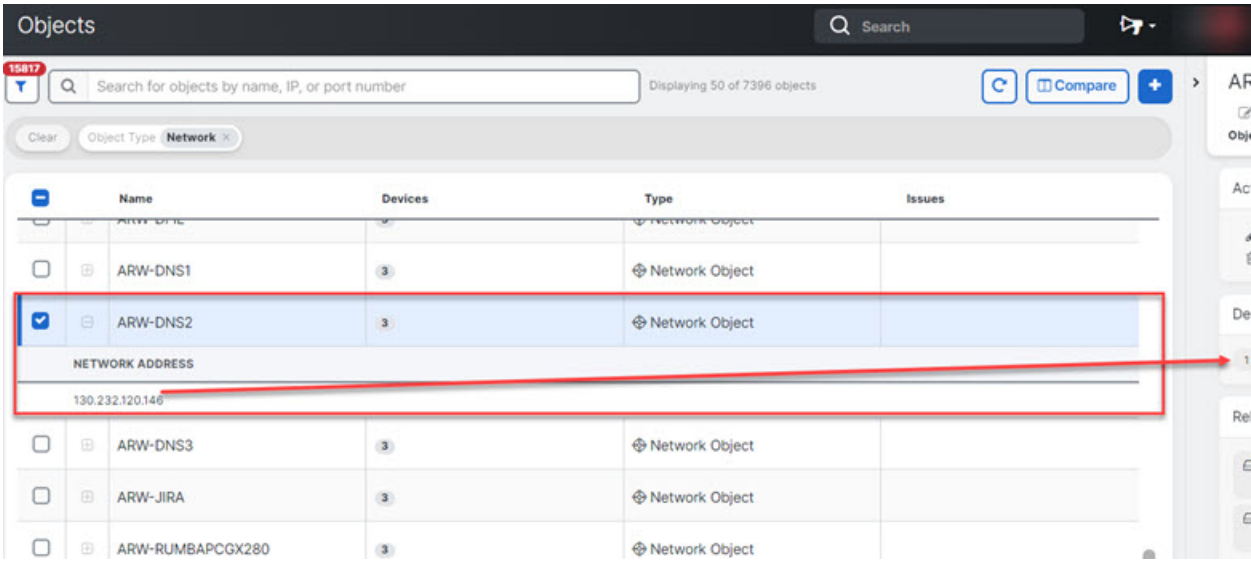
Object	Description
Create IP Address Pool	Address pool objects can be configured to match against an individual IPv4 or IPv6 address or an IP address range.
Upload RA VPN AnyConnect Client Profile	AnyConnect Client Profile objects are file objects and represent files used in configurations, typically for remote access VPN policies. They can contain an AnyConnect Client Profile and AnyConnect Client Image files.
Network Objects	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
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.
ASA Time Range Objects	A time range object defines a specific time consisting of a start time, an end time, and optional recurring entries. You use these objects in network policies to provide time-based access to certain features or assets.
Trustpoint Objects	Trustpoints let you manage and track digital certificates in ASA.

Shared Objects

Cisco Defense Orchestrator (CDO) 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, CDO shows you the contents of the object in the object table. Shared objects have exactly the same contents. CDO 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.



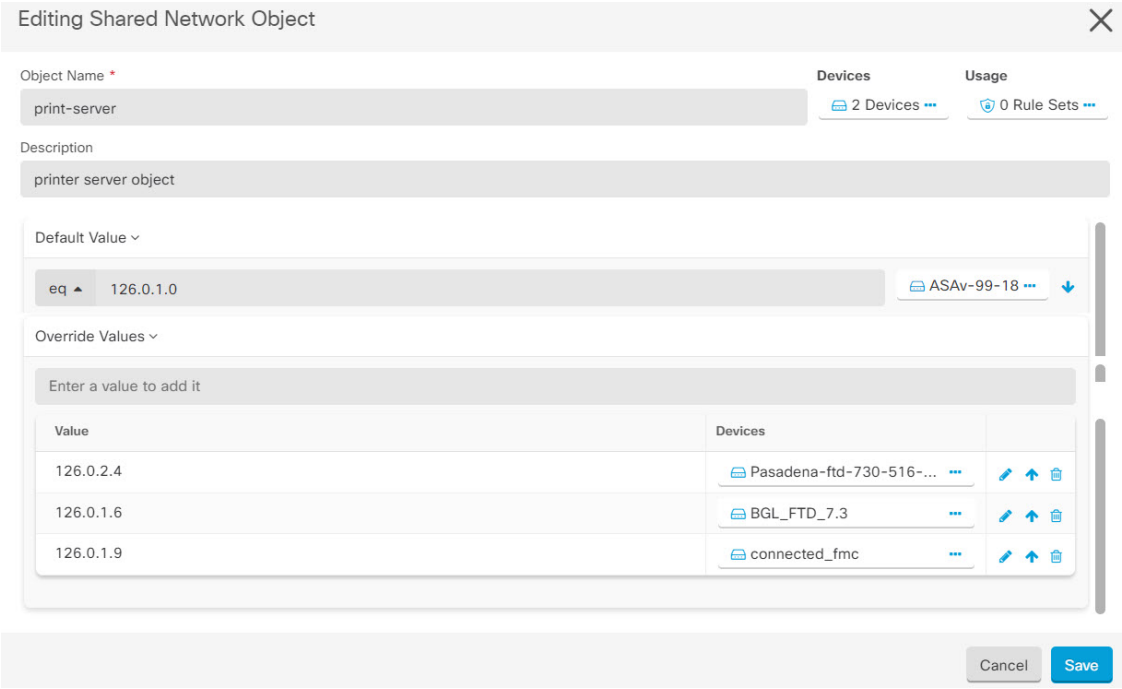
Object Overrides

An object override allows you to override the value of a shared network object on specific devices. CDO 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, CDO 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 242.



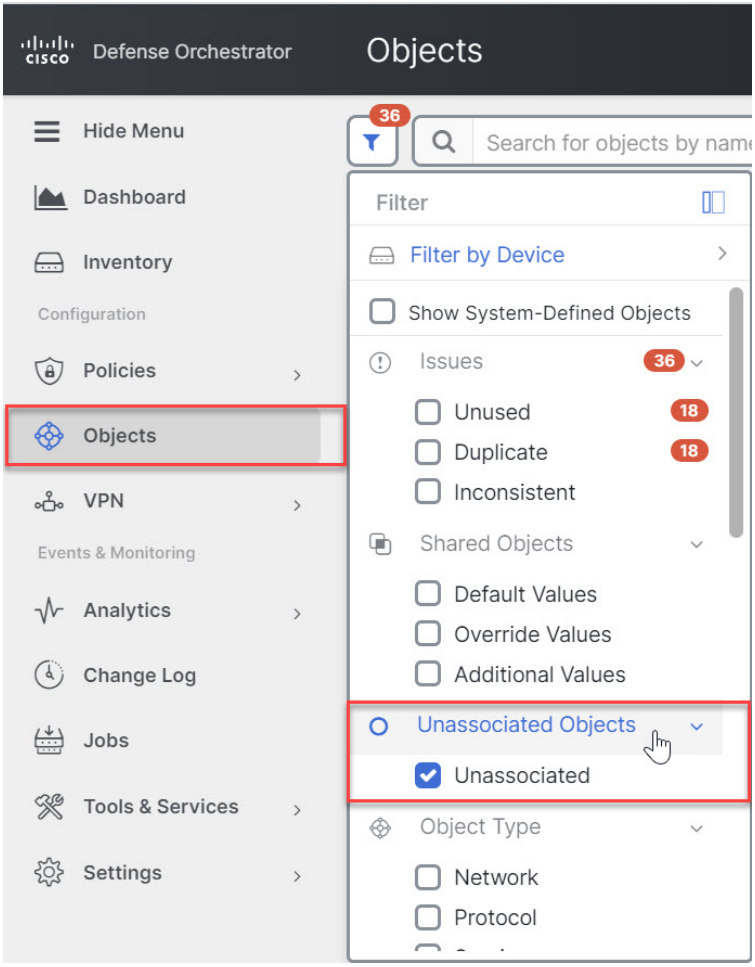
Note If there are inconsistent objects, you can combine them into a single shared object with overrides. For more information, see Resolve Inconsistent Object Issues, on page 502.

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, CDO 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 CDO as a copy to ensure that not all configurations are lost if the rule or policy associated with the object is deleted accidentally.

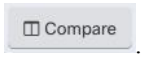
To view unassociated objects click in the left-hand pane of the Objects tab and check the **Unassociated** checkbox.



Compare Objects

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. CDO 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:

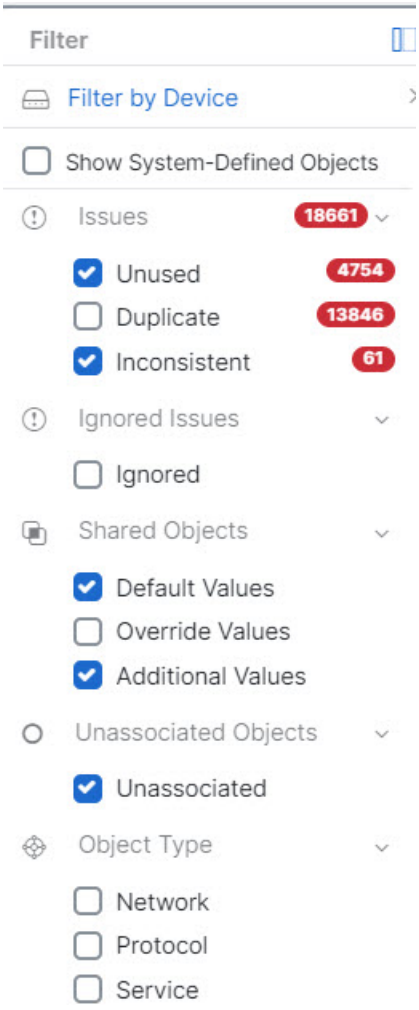
The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

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 CDO 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.

Step 1 In the left pane, click **Objects** and choose an option.

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 CDO 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 CDO 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.

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 > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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.

Step 1 In the left pane, choose **Objects** and choose an option.

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.

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 CDO.

Note that not all platforms support network objects, such as Cisco Merkai and Multicloud Defense; when you share dynamic objects, CDO automatically translates the appropriate information from the originating platform or device into a set of usable information that CDO 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
ASA	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
ASA	Yes	Yes	Yes
Multicloud Defense	Yes	Yes	Yes

Reusing Network Objects Across Products

If you have a Cisco Defense Orchestrator tenant with a cloud-delivered Firewall Management Center and one or more on-prem 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-Prem Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the on-prem management center on which you want to use the object and discard the ones that you do not want. Navigate **Tools & Services** > **Firewall Management Center**, select the on-prem management center, and click **Objects** to see your objects in the On-Prem 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 Cisco Defense Orchestrator
- 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 CDO objects page if they are used in policies that were deployed to FTD devices.

- Sharing Network Objects between CDO 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 CDO Customers Open a Support Ticket with TAC to have the features enabled on your tenant.
- Sharing network objects between CDO and On-Prem Management Center is not automatically enabled on CDO for new on-prem management centers onboarded to CDO. If your network objects are not being shared with On-Prem Management Center, ensure **Discover & Manage Network Objects** toggle button is enabled for the on-prem management center in **Settings** or How CDO Customers Open a Support Ticket with TAC to have the features enabled on your tenant.

Viewing Network Objects

Network objects you create using CDO and those CDO 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.

Create or Edit ASA Network Objects and Network Groups

An ASA network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects, network groups, and IP addresses that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using CDO.

Table 6: Pemitted Values of ASA Network Objects and Groups

Device type	IPv4 / IPv6	Single Address	Range of addresses	Partially Qualified Domain Name (PQDN)	Subnet using CIDR Notation
ASA	IPv4 / IPv6	Yes	Yes	Yes	Yes

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-prem 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 > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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.

Create an ASA Network Object

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 objects are used in access rules, network policies, and NAT rules. You can create, update, and delete network objects and network groups using CDO.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-prem management center on which you want these objects.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click the blue plus button to create an object.

Step 3 Click **ASA** > **Network**.

Step 4 Enter an object name.

Step 5 Select **Create a network object**.

Step 6 (optional) Enter an object description.

Step 7 In the **Value** section, add the IP address information in one of these ways:

- Select **eq** and then enter a single IP address, a subnet address using CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and then enter a range of IP addresses. Enter the range with the beginning and ending address in the range separated by a space. For example, 10.1.1.1 10.1.1.255 or 2001:DB8:1::1 2001:DB8:1::3

Step 8 Click **Add**.

Important The newly created network objects aren't associated with any ASA 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 Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create an ASA Network Group

A **network group** can contain IP address values, network objects, and network groups. When you are creating 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. Network groups can contain both IPv4 and IPv6 addresses.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-prem management center on which you want these objects.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click the blue plus button to create an object.

Step 3 Click **ASA** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network group**.

Step 6 (optional) Enter an object description.

Step 7 In the **Values** field, enter a value or object name. When you start typing, CDO provides object names or values that match your entry.

Step 8 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 9 If CDO finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 10 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 check mark 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 check mark to save it.
- Click **Add Value** to create an inline value without using an object. Enter a value and click the check mark 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 11 After adding the required objects, click **Add** to create a new network group.

Step 12 Preview and Deploy Configuration Changes for All Devices, on page 233.

Edit an ASA 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 > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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.

Step 1 In the left pane, click **Objects > ASA 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 in the procedures above.

Note Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. CDO 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 an ASA 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 > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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.

Step 1 In the left pane, click **Objects > ASA 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 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 5 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, CDO 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 CDO 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.
- Click **Add Value** to create an inline value without using an object. Enter a value 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 6 Click **Save**. CDO displays the policies that will be affected by the change.

Step 7 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 8 Preview and Deploy Configuration Changes for All Devices, on page 233.

Add Additional Values to a Shared Network Group in CDO

The values in a shared network group that are present on all devices associated with it are called "default values". CDO 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 CDO 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 it 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 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 > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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.

Step 1 In the left pane, click **Objects > ASA 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, CDO 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 CDO 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.
- Click **Add Value** to create an inline value without using an object. Enter a value 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**. CDO 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, on page 233.

Edit Additional Values in a Shared Network Group in CDO

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > ASA 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-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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.

Step 1 In the left pane, click **Objects > ASA 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**. CDO 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, on page 233.

Deleting Network Objects and Groups in CDO

If Cloud-delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the or **Objects > ASA Objects** page deletes the replicated network object or group from the **Objects > Other FTD Objects** page and vice-versa.

Trustpoint Objects

CDO allows you to add digital certificates as trustpoint objects and then install them on one or multiple managed ASA devices. A single trustpoint object is a container that holds an identity pair (identity certificate and issuer's CA certificate), identity certificate only, or CA certificate only.

You can configure many trustpoints in an ASA device. The supported certificate formats are PKCS12, PEM, and DER.

Adding an Identity Certificate Object Using PKCS12

This procedure creates an internal certificate identity or internal identity certificate by uploading a certificate file or pasting existing certificate text into a text box. You can generate as many identity certificates as you want.

You can upload a file encoded in **PKCS12** format. A PKCS12 is a single file that holds the CA server certificate, any intermediate certificates, and the private key in one encrypted file. A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file. Enter the **Passphrase** value for decryption.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click  and select **ASA** > **Trustpoints**.

Step 3 Enter an **Object 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 4 In the **Certificate Type** step, select **Identity Certificate**.

Step 5 In the **Import Type** step, select **Upload** to upload the certificate file.

The **Enrollment** step is set to Terminal.

Step 6 In the **Certificate Contents** step, enter the PKCS12 format details.

A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file. Enter the **Passphrase** value for decryption.

Step 7 Click **Continue**.

Step 8 In the **Advanced Options** step, you can configure the following:

In the **Revocation** tab, you can configure the following:

- **Enable Certificate Revocation Lists (CRL)** — Check to enable CRL checking.

  By default the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

  Cache Refresh Time (in minutes) — Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

- **Enable Online Certificate Status Protocol (OCSP)** — Check to enable OCSP checking.

OCSP Server URL—The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with `http://`.

Disable Nonce Extension — Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

Evaluation Priority — Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

- **Consider the certificate valid if revocation information cannot be reached**— Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

  For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Click the **Others** tab:

- **Use CA Certificate for the Validation of** — Specify the type of connections that can be validated by this CA.
  - **IPSec Client** — Validates certificate presented by remote SSL servers.
  - **SSL Client** — Validates certificates presented by incoming SSL connections.
  - **SSL Server** — Validates certificates presented by incoming IPSec connections.
- **Use Identity Certificate for** — Specify how the enrolled ID certificate can be used.
  - **SSL & IPSec** — Use for authenticating SSL & IPSec connections
  - **Code Signer** — Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.
- **Other Options**:
  - **Enable CA flag in basic constraints extension** — Select this option if this certificate should be able to sign other certificates. The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate i
  - **Accept certificates issued by this CA** — Select this option to indicate that the ASA should accept certificates from the specified CA.
  - **Ignore IPSec Key Usage** — Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

Step 9 Click **Add**.

Creating a Self-Signed Identity Certificate Object

This procedure describes steps for generating a self-signed certificate for your ASA by entering the appropriate certificate field values in a wizard. You can generate as many self-signed certificates as you want.

To create a Self-Signed identity certificate object, perform the following steps:

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click  and select **ASA** > **Trustpoints**.

Step 3 Enter an **Object 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 4 In the **Identity Certificate** step, select **Identity Certificate**.

Step 5 In the **Import Type** step, select **New** to upload the certificate file and click **Continue**.

Step 6 In the **Enrollment** step, select **Self-Signed** and click **Continue**.

The **Certificates Content** step appears. Read Self-Signed and CSR Certificate Generation Based on Certificate Contents to understand the CN and SANS content in the Self-Signed certificate that is being generated.

Step 7 In the **Certificate Contents** step, configure the following:

- **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.
- **Email Address (EA)**— The e-mail address associated with the identity certificate.
- **IP Address**— The ASA IP address on the network in four-part, dotted-decimal notation.
- **Device's FQDN**— An unambiguous domain name, to indicate the position of the node in the DNS tree hierarchy.
- **Include Device's Serial Number**— Select the check box if you want to add the ASA serial number to the certificate parameters.

a) Click the **Key** tab.

- Choose the **RSA** or **ECDSA** key type.
- **Key Size**: If the key pair does not exist, defines the desired key size (modulus), in bits. The recommended key size for RSA is 1024 and for ECDSA is 348. The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.
- Click **Continue**.

Step 8 In the **Advanced Options** step, you can configure the following:

In the **Revocation** tab, you can configure the following:

- **Enable Certificate Revocation Lists (CRL)** — Check to enable CRL checking.

  By default the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

  Cache Refresh Time (in minutes) — Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

- **Enable Online Certificate Status Protocol (OCSP)** — Check to enable OCSP checking.

  OCSP Server URL—The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with `http://`.

  Disable Nonce Extension — Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

  Evaluation Priority — Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

- **Consider the certificate valid if revocation information cannot be reached**— Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

  For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Click the **Others** tab:

- **Use CA Certificate for the Validation of** — Specify the type of connections that can be validated by this CA.
  - **IPSec Client** — Validates certificate presented by remote SSL servers.
  - **SSL Client** — Validates certificates presented by incoming SSL connections.
  - **SSL Server** — Validates certificates presented by incoming IPSec connections.
- **Use Identity Certificate for** — Specify how the enrolled ID certificate can be used.
  - **SSL & IPSec** — Use for authenticating SSL & IPSec connections
  - **Code Signer** — Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.
- **Other Options**:
  - **Enable CA flag in basic constraints extension** — Select this option if this certificate should be able to sign other certificates. The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate i
  - **Accept certificates issued by this CA** — Select this option to indicate that the ASA should accept certificates from the specified CA.

- **Ignore IPSec Key Usage** — Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

Step 9 Click **Add**.

Adding an Identity Certificate Object for Certificate Signing Request (CSR)

The Certification Authority (CA) server information and enrollment parameters are required to generate Certificate Signing Requests (CSRs) and obtain Identity Certificates from the specified CA. You need to select either Rivest-Shamir-Adleman (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) key type to generate the request.

Create a trustpoint object by providing identification information and optionally uploading a CA certificate obtained from a CA.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click  and select **ASA** > **Trustpoints**.

Step 3 Enter an **Object 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 4 In the **Identity Certificate** step, select **Identity Certificate**.

Step 5 In the **Import Type** step, select **New** to upload the certificate file and click **Continue**.

Step 6 In the **Enrollment** step, select **Manual**.

Step 7 (optional) You can paste or upload the CA certificate obtained from your CA. You can leave the field empty.

Step 8 Click Continue.

The Certificates Content step appears. Read Self-Signed and CSR Certificate Generation Based on Certificate Contents to understand the CN and SANS content in the Signed certificate that is being generated.

Step 9 In the **Certificate Contents** step, configure the following:

- **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.
- **Email Address (EA)**— The e-mail address associated with the identity certificate.
- **IP Address**— The ASA IP address on the network in four-part, dotted-decimal notation.

- **Subject Alternative Name (SAN)**— This field will be part of Certificate Subject DN as 'unstructuredName' as well. We recommend you use this field if the certificate is used for multiple domains or IP addresses.
  - **Use Device Host Name:** Host name of the device is used.
  - **Custom: Device's FQDN**— An unambiguous domain name, to indicate the position of the node in the DNS tree hierarchy.

    Note We recommend the values specified in CN and **Custom FQDN** are the same.

- **Include Device's Serial Number**— Select the check box if you want to include the serial number of ASA in the certificate. The CA uses the serial number to either authenticate certificates or to later associate a certificate with a particular device. If you are in doubt, include the serial number, as it is useful for debugging purposes.

a) Click the **Key** tab.

- Choose the **RSA** or **ECDSA** key type.
- **Key Size**: If the key pair does not exist, defines the desired key size (modulus), in bits. The recommended key size for RSA is 1024 and for ECDSA is 348. The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.
- Click **Continue**.

Step 10 In the **Advanced Options** step, you can configure the following:

In the **Revocation** tab, you can configure the following:

- **Enable Certificate Revocation Lists (CRL)** — Check to enable CRL checking.

  By default the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

  Cache Refresh Time (in minutes) — Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

- **Enable Online Certificate Status Protocol (OCSP)** — Check to enable OCSP checking.

  OCSP Server URL—The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with **`http://`**.

  Disable Nonce Extension — Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

  Evaluation Priority — Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

- **Consider the certificate valid if revocation information cannot be reached**— Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

  For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Click the **Others** tab:

- **Use CA Certificate for the Validation of** — Specify the type of connections that can be validated by this CA.
  - **IPSec Client** — Validates certificate presented by remote SSL servers.
  - **SSL Client** — Validates certificates presented by incoming SSL connections.
  - **SSL Server** — Validates certificates presented by incoming IPSec connections.
- **Use Identity Certificate for** — Specify how the enrolled ID certificate can be used.
  - **SSL & IPSec** — Use for authenticating SSL & IPSec connections
  - **Code Signer** — Code signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.
- **Other Options**:
  - **Enable CA flag in basic constraints extension** — Select this option if this certificate should be able to sign other certificates. The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate i
  - **Accept certificates issued by this CA** — Select this option to indicate that the ASA should accept certificates from the specified CA.
  - **Ignore IPSec Key Usage** — Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

Step 11 Click **Add**.

This creates a trustpoint certificate object.

Adding a Trusted CA Certificate Object

Obtain a trusted CA certificate from an external certificate authority, or create one using your own internal CA, for example, with OpenSSL tools. You can upload a file encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click  and select **ASA** > **Trustpoints**.

Step 3 Enter an **Object 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 4 In the **Certificate Type** step, select **Trusted CA Certificate**.

Step 5 In the **Certificate Contents** step, paste the certificate contents in the text box or upload the CA certificate file as explained in the wizard.

Step 6 Click **Continue**. The wizard advances to step 4.

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 7 In the **Advanced Options** step, you can configure the following:

In the **Revocation** tab, you can configure the following:

- **Enable Certificate Revocation Lists (CRL)** — Check to enable CRL checking.

  By default the **Use CRL distribution point from the certificate** check box is selected to obtain the revocation lists distribution URL from the certificate.

  Cache Refresh Time (in minutes) — Enter the number of minutes between cache refreshes. The default is 60 minutes. The range is 1-1440 minutes. To avoid having to retrieve the same CRL from a CA repeatedly, the ASA can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the ASA removes the least recently used CRL until more space becomes available.

- **Enable Online Certificate Status Protocol (OCSP)** — Check to enable OCSP checking.

  OCSP Server URL—The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with **`http://`**.

  Disable Nonce Extension — Enable the check box which cryptographically binds requests with responses to avoid replay attacks. This process works by matching the extension in the request to that in the response, ensuring that they are the same. Uncheck the **Disable Nonce Extension** check box if the OCSP server you are using sends pregenerated responses that do not include this matching nonce extension.

  Evaluation Priority — Specify whether to evaluate the revocation status of a certificate first in CRL or OSCP.

- **Consider the certificate valid if revocation information cannot be reached**— Select this check box to consider the certificate to be a valid certificate if revocation information is unreachable.

  For more information on revocation check, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Click the **Others** tab:

- **Use CA Certificate for the Validation of** — Specify the type of connections that can be validated by this CA.
  - **IPSec Client** — Validates certificate presented by remote SSL servers.
  - **SSL Client** — Validates certificates presented by incoming SSL connections.
  - **SSL Server** — Validates certificates presented by incoming IPSec connections.
- **Other Options**:
  - **Enable CA flag in basic constraints extension** — Select this option if you want to validate if the subject of the certificate is a CA using the basic constraints extension.
  - **Accept certificates issued by this CA** — Select this option to indicate that the ASA should accept certificates from the specified CA.
  - **Accept certificates issued by the subordinates CAs of this CA** — Select this option to indicate that the ASA should accept certificates from the subordinate CA.
  - **Ignore IPSec Key Usage** — Select this option if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

Step 8 Click **Add**.

This creates a trustpoint certificate object.

Self-Signed and CSR Certificate Generation Based on Certificate Contents

You need to have an idea of the CN and SANS content in the Self-Signed and CSR certificates. The content is based on the parameters you specify during their creation. You need to configure the parameters precisely for the AnyConnect clients to connect to the intended VPN headends of your organization.

This section provides different use cases with examples to give you an idea of the content of Self-Signed and CSR certificates based on the parameters specified.

Usecase 1: Different CN and FQDN values

Example:

- Common Name (CN): mywebsite.com
- FQDN: mysan.com

Table 7: Example: Different CN and FQDN values

	Common Name	unstructuredName	SANS
Self-Signed	mywebsite.com	mysan.com	mysan.com
CSR	mywebsite.com	mysan.com	-

Usecase 2: FQDN field set to None

Example:

- Common Name (CN): mywebsite.com
- FQDN: None

Table 8: Example: FQDN field set to None

	Common Name	SANS
Self-Signed	Host Name	-
CSR	mywebsite.com	-

Usecase 3: No FQDN (Default FQDN)

Example:

- Common Name (CN): mywebsite.com

Table 9: Example: No FQDN (Default FQDN)

	Common Name	unstructuredName	SANS
Self-Signed	mywebsite.com	Host Name	-
CSR	mywebsite.com	Host Name	Host Name

Usecase 4: IP Address is specified in FQDN

Example:

- Common Name (CN): mywebsite.com
- FQDN: 4.5.6.7

Table 10: Example: IP Address is specified in FQDN

	Common Name	unstructuredName	SANS
Self-Signed	mywebsite.com	4.5.6.7	-
CSR	mywebsite.com	4.5.6.7	4.5.6.7

Usecase 5: IP Address is Specified

Example:

- IP Address: 4.5.6.7
- Common Name (CN): mywebsite.com
- FQDN: fqdn.com

Table 11: Example: IP Address is specified

	Common Name	unstructuredAddress	unstructuredName	SANS
Self-Signed	mywebsite.com	4.5.6.7	fqdn.com	-
CSR	mywebsite.com	4.5.6.7	fqdn.com	fqdn.com

Usecase 6: Serial Number Check box is Selected

Example:

- Serial Number: 9AQXMWOKDT9

Table 12: Example: IP Serial Number Check box is Selected

	serialNumber	SANS
Self-Signed	9AQXMWOKDT9	-
CSR	9AQXMWOKDT9	fqdn.com

Usecase 7: Email Address is Specified

Example:

- EA: abc@xyz.com

Table 13: Example: Email Address is Specified

	unstructredName	emailAddress	SANS
Self-Signed	Host Name	abc@xyz.com	Host Name
CSR	Host Name	abc@xyz.com	-

RA VPN Objects

Service Objects

ASA Service Objects

ASA service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the IP protocol suite. In a service object you can specify a single protocol and assign it to a source port, destination port, or both source and destination ports. A service group contains many service objects and can include a mix of protocols.

A port group is a kind of ASA service object. Port groups contain port objects that pair a service type, such as TCP or UDP, and a port number or a range of port numbers. You can then use the objects in security policies for the purposes of defining traffic matching criteria. For example, you can use them in access control rules to allow traffic to a specific range of TCP ports.

See Create and Edit ASA 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. CDO 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.

ICMP Objects

An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. CDO recognizes these objects in ASA and Firepower configurations when those devices are onboarded and CDO gives them their own filter of "ICMP" so you can find the objects easily.

Using CDO, you can rename or remove ICMP objects from an ASA configuration. You can use CDO 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.

Related Information:

- Deleting Objects, on page 101

Create and Edit ASA Service Objects

In a service object, you can specify a single protocol and assign it to a source port, destination port, or both source and destination ports.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click **Create Object** > **ASA** > **Service**.

Step 3 Enter an object name.

Step 4 Select **Create a service object**

Step 5 Click the **Service Type** button and select the protocol for which you want to make an object.

- **For TCP, UDP, and TCP-UDP service types,** enter a source port, destination port, or both:
  - The source port identifier allows you to match traffic originating from a particular numbered port. In the source port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.
  - The destination port identifier allows you to match traffic arriving at a particular numbered port. In the destination port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.
- **For Protocol service types**, enter a protocol number between 0-255, or a well-known name, such as ip, tcp, udp, gre, and so forth.

Step 6 Click **Add**.

Examples

- A service object that identifies incoming FTP traffic would be one with a TCP Service type and a destination port range of 21.
- A service object that identifies outgoing DNS and DNS over TCP traffic would be one with a tcp-udb service type and a source port equal to 53.

Create an ASA Service Group

A service group can be made up of one or more service objects representing one or more protocols.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click **Create Object** > **ASA** > **Service**.

Step 3 Enter an object name.

Step 4 Select **Create a service 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 If needed, add an extra individual service type value to the service group

- **For TCP, UDP, and TCP-UDP service types,** enter a source port, destination port, or both:
  - The source port identifier allows you to match traffic originating from a particular numbered port. In the source port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.
  - The destination port identifier allows you to match traffic arriving at a particular numbered port. In the destination port identifier, select an operator: equal to, range, less than, greater than, or not equal to and provide the appropriate port number or range.
- **For Protocol service types**, enter a protocol number between 0-255, or a well-known name, such as ip, tcp, udp, gre, and so forth.

Step 7 To add more individual port values, click **Add Another Value** and repeat step 6.

Step 8 Click **Add** when you are done adding service objects and service values to the service group.

Edit an ASA Service Object or Service Group

Step 1 In the left pane, click **Objects > ASA 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 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 CDO 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.

ASA Time Range Objects

What is a Time Range Object?

A time range object defines a specific time consisting of a start time, an end time, and optional recurring entries. You use these objects in network policies to provide time-based access to certain features or assets. For example, you could create an access rule that allows access to a particular server during working hours only. Creating a time range does not restrict access to the device. Note that the times configured for these objects are local to the device.

You can add an absolute or recurring time ranges to this object. Recurring ranges are considered to be periodic time ranges.

Note If a time range has both absolute and periodic values specified, then the periodic values are evaluated only after the absolute start time is reached and they are not further evaluated after the absolute end time is reached.

Create an ASA Time Range Object

Use the following procedure to create a time range object for an ASA device:

Step 1 In the left pane, click **Objects** > **ASA Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **ASA** > **Time Range**.

Step 4 Enter an object name.

Step 5 Define a time range.

- Absolute Time Range - Enter a Start Time and an End Time for the desired time range; you can choose to execute this object over a matter of minutes, hours, days, or weeks. A time range object can only have one absolute time range.
- Recurring Time Ranges - click the  to add a periodic time range that will repeat throughout the week. Select the **Frequency** from the drop-down menu, the **Days** of the week the time range should go into effect, and the **Start** and **End** times. A time range object can have multiple periodic ranges.

Note The **start** and **end** times for a time range object are optional. If an object has no start time established, the time range goes into effect immediately. If an object has no end time established, the time range lasts indefinitely.

Step 6 Click **Add** to create the object.

Edit an ASA Time Range Object

Use the following procedure to edit a time range object for an ASA device:

Step 1 In the left pane, click **Objects > ASA 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 edit  .

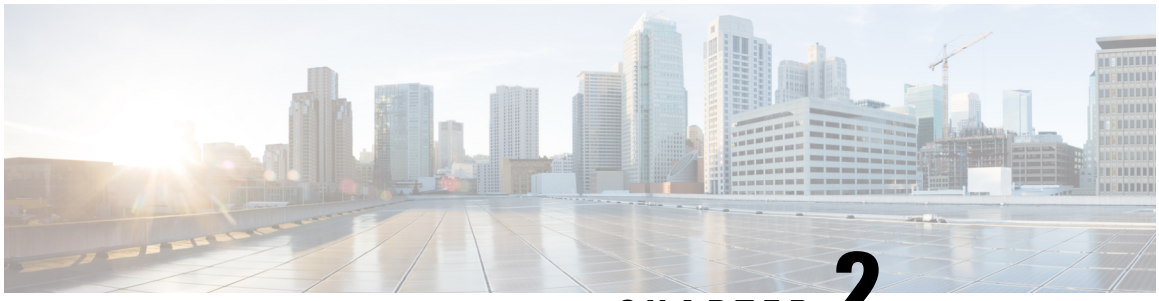
Step 4 Edit the values as needed and click **Save**.

Step 5 If the object is currently used by any policies, CDO 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 6 If the object is used in a policy on a device, 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
- Manage ASA Network Security Policy



CHAPTER 2

Onboard Devices and Services

You can onboard both live devices and model devices to CDO. Model devices are uploaded configuration files that you can view and edit using CDO.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect CDO to the device or service.

See Secure Device Connector, on page 8 for more information on the SDC and its state.

This chapter covers the following sections:

Onboard ASA Device to CDO

Use this procedure to onboard a single live ASA device, not an ASA model, to CDO. If you want to onboard multiple ASAs at once, see Onboard Multiple ASAs to CDO.

Before you begin

Device Prerequisites

- Review Connect CDO to your Managed Devices, on page 9.
- Device must be running at least version 8.4+.

Note TLS 1.2 was not available for the ASA management-plane until version 9.3(2). With version 9.3(2), a local SDC is required to onboard to CDO.

- The running configuration file of your ASA must be less than 4.5 MB. To confirm the size of your running configuration file, see Confirming ASA Running Configuration Size.
- IP addressing: Each ASA, ASAv, or ASA security context must have a unique IP address and the SDC must connect to it on the interface configured to receive management traffic.

Certificate Prerequisites

If your ASA device does not have a compatible certificate, onboarding the device may fail. Ensure the following requirements are met:

- The device uses a TLS version equal to or greater than 1.0.
- 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).
- The certificate must be a SHA-256 certificate. SHA1 certificates are not accepted.
- 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.

If you experience certificate errors during the onboarding process, see Cannot onboard ASA due to certificate error, on page 467for more information.

Open SSL Cipher Prerequisites

If the device does not have a compatible SSL cipher suite, the device cannot successfully communicate to the Secure Device Connector (SDC). Use any of the following cipher suites:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256

- DHE-RSA-AES256-SHA256

If the cipher suite you use on your ASA is not in this list, the SDC does not support it and you will need to Updating your ASA's Cipher Suite.

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the blue plus button  to onboard an ASA.

Step 3 Click the **ASA** tile.

Step 4 In the **Locate Device** step, perform the following:

a. Click the **Secure Device Connector** button and select a Secure Device Connector installed in your network. If you would rather not use an SDC, CDO can connect to your ASA using the Cloud Connector. Your choice depends on how you Connect CDO to your Managed Devices.

b. Give the device a name.

c. Enter the location (IP address, FQDN, or URL) of the device or service. The default port is 443.

d. Click **Next**.

Step 5 In the **Credentials** step, enter the username and password of the ASA administrator, or similar highest-privilege ASA user, that CDO will use to connect to the device and click **Next**.

Step 6 (Optional) In the Done step, enter a label for the device. You will be able to filter your list of devices by this label. See CDO Labels and Filtering for more information.

Step 7 After labeling your device or service, 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.

Onboard a High Availability Pair of ASA Devices to CDO

When onboarding an ASA that is part of a high-availability pair, use Onboard ASA Device to CDO, on page 127 to onboard only the primary device of the pair.

Onboard an ASA in Multi-Context Mode to CDO

About Multi-Context Mode

You can partition a single ASA, installed on a physical appliance, into multiple logical devices known as contexts. There are three kinds of configurations used in an ASA configued in multi-context mode:

- Security Context
- Admin Context
- System Configuration

About Security Contexts

Each security context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple security contexts are similar to having multiple standalone devices. A security context is not a virtual ASA in the sense of a virtual machine image installed in a private cloud infrastructure. A security context is configured on an ASA installed on a hardware appliance. Each context is configured on a physical interface of that appliance.

See the ASA CLI and ASDM configuration guides for more information about multi-context mode.

CDO onboards each security context as a separate ASA and manages it as if it were a separate ASA.

About Admin Contexts

The admin context is like a security context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users.

CDO onboards each admin context as a separate ASA and manages it as if it were a separate ASA. CDO also uses the admin context when upgrading ASA and ASDM software on the appliance.

About System Configuration

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the *admin context*.

CDO does not onboard the system configuration.

Onboarding Prerequisites for Security and Admin Contexts

The prerequisites for onboarding security and admin contexts are the same for onboarding any other ASA. See Onboard ASA Device to CDO, on page 127for the list of prerequisites.

To learn which Cisco appliances support ASAs in multi-context mode, see the "Multiple Context Mode" chapter in the *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide* for whatever ASA software version you are running.

For an ASA running as a single context firewall and for the admin context of a multiple-context firewall, many different port numbers could be used for ASDM and CDO access. However, for security contexts, the ASDM and CDO access port is fixed to port 443. This is a limitation of ASA.

Onboarding ASA Security and Admin Contexts

The method of onboarding a security context or admin context is the same for onboarding any other ASA. See Onboard ASA Device to CDO, on page 127 or Onboard Multiple ASAs to CDO, on page 131 for onboarding instructions.

Upgrading Security Contexts

CDO treats each security and admin context of a multiple-context ASA as a separate ASA and each is onboarded separately. However, all security and admin contexts of a multiple-context ASA run the same version of ASA software installed on the appliance.

To upgrade the versions of ASA and ASDM used by the ASA's security contexts, you onboard the the admin context and perform the upgrade on that context. See Upgrade ASA and ASDM Images on a Single ASA, on page 138 or Upgrade Bulk ASA and ASDM in CDO, on page 135 Upgrade Bulk ASA and ASDM in CDO, on page 135for more information.

Onboard Multiple ASAs to CDO

CDO allows you to bulk onboard ASAs by providing the necessary information for all the ASAs in a .csv file. As the ASAs are being onboarded, you can use the filter pane to show which onboarding attempts are queued, loading, complete, or have failed.

Before you begin

- Review Connect CDO to your Managed Devices, on page 9.
- Prepare a .csv file with the connection information of the ASAs you want to onboard. Add the information about one ASA on its own line. You can use a # at the beginning of a line to indicate a comment.
  - ASA location (either IP address or FQDN)
  - ASA administrator username
  - ASA administrator password
  - (Optional) Device name for CDO
  - In the SDCName field, specify the name of a Secure Device Connector (SDC) in your network you want to use to connect CDO to your ASA. You can also enter "none" if you are not going to connect your ASA to CDO using an SDC. When onboarding the device, specifying "none" in SDCName field, onboards the ASA using the Cloud Connector. The Cloud Connector allows you to connect your device to CDO without installing an SDC. Your choice depends on how you Connect CDO to your Managed Devices.
  - (Optional) Device labels for CDO
  - To add one label, add the label name to the last CSV field.
  - To add more than one label to a device, surround the values with quotes. For example, `alpha,beta,gamma`.
  - To add a category and choice label, separate the two values with a colon (:). For example, `Rack:50`.

Sample of the configuration file:

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

Caution CDO does not validate any of the data in the .csv file. You need to ensure the accuracy of the entries.

Step 1 In the navigation bar, click **Inventory**

Step 2 Click the blue plus button to onboard an ASA.

Step 3 On the Onboarding page, click the **Multiple ASAs** tile.

Step 4 Click **Browse** to locate the .csv file containing your ASA entries. The devices you specified are now queued in the ASA Bulk Onboarding table ready to be onboarded.

Caution Do not navigate away from the ASA Bulk Onboarding page until the onboarding process is complete. Navigating away stops the onboarding process.

Step 5 Click **Start**. You will see the progress of the onboarding process in the status column of the ASA Bulk Onboarding table. After the device have been successfully onboarded you will see their status change to "Complete."

What to do next

If you need to pause bulk onboarding and resume it later, see Pause and Resume Onboarding Multiple ASAs, on page 132

.

Pause and Resume Onboarding Multiple ASAs

If you need to pause the onboarding process, click **Pause**. CDO finishes onboarding any device it started onboarding. To resume the bulk onboarding process, click **Start**. CDO will start onboarding the next queued device.

If you click **Pause** and navigate away from this page, you will need to return to the page and follow the bulk onboarding procedure again from the beginning. However, CDO recognizes the devices it has already onboarded, marks the devices from this new onboarding attempts as duplicates, and quickly moves through the list to onboard the queued devices.

Create and Import an ASA Model to CDO

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab.

Step 4 Select an ASA device and in the **Management** on the left pane, click **Configuration**.

Step 5 Click **Download** to download the device configuration to your local computer.

Import ASA Configuration

Attention: The ASA running configuration file you are onboarding must be less than 4.5 MB. Confirm the size of the configuration file before you onboard it.

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the blue plus ( ) button to import the configuration.

Step 3 Click on **Import configuration for offline management**.

Step 4 Select the **Device Type** as **ASA**.

Step 5 Click **Browse** and select the configuration file (text format) to upload.

Step 6 Once the configuration is verified, you're prompted to label the device or service. See CDO Labels and Filtering for more information.

Step 7 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 CDO

Use the following procedure to delete a device from CDO:

Step 1 Log into CDO.

Step 2 Navigate to the **Inventory** page.

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.

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. CDO also refers to these uploaded configuration files as "models."

You can import the configurations of these devices to CDO:

- Adaptive Security Applicance (ASA). See Create and Import an ASA Model to CDO.
- Cisco IOS devices like the Aggregation Services Routers (ASR) and Integrated Services Routers (ISRs).

Prerequisites for ASA and ASDM Upgrade in CDO

Cisco Defense Orchestrator provides a wizard that helps you upgrade the ASA and ASDM images installed on an individual ASA, multiple ASAs, ASAs in an active-standby configuration, and ASAs running in single-context or multi-context mode.

CDO maintains a repository of ASA and ASDM images that you can upgrade to. When you choose your upgrade images from CDO's image repository, CDO performs all the necessary upgrade steps behind the scenes. The wizard guides you through the process of choosing compatible ASA software and ASDM images, installs them, and reboots the device to complete the upgrade. We secure the upgrade process by validating that the images you chose on CDO are the ones copied to, and installed on, your ASA. CDO periodically reviews its inventory of ASA binaries and adds the newest ASA and ASDM images to its repository when they are available. This is the best option for customers whose ASAs have outbound access to the internet.

CDO's image repository only contains generally available (GA) images. If you do not see a specific GA image in the list, please contact Cisco TAC or email support from the **Contact Support** page. We will process the request using the established support ticket SLAs and upload the missing GA image.

If your ASAs do not have outbound access to the internet, you can download the ASA and ASDM images you want from Cisco.com, store them in your own repository, provide the upgrade wizard with a custom URL to those images, and CDO performs upgrades using those images. In this case, however, you determine what images you want to upgrade to. CDO does not perform the image integrity check or disk-space check. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB.

Configuration Prerequisites for All ASAs

- DNS needs to be enabled on the ASA.
- ASA should be able to reach the internet if you use upgrade images from CDO's image repository.
- Ensure HTTPS connectivity between the ASA and the repository FQDN.
- The ASA has been successfully onboarded to CDO.
- The ASA is synced to CDO.
- The ASA is online.
- For custom URL upgrades:
  - Use the Cisco ASA Upgrade Guide to determine what version of ASA and ASDM are compatible with your ASAs.
  - Download the ASA and ASDM images to your image repository.
  - Ensure that the ASA has access to your image repository.
  - Ensure you have enough disk space on your ASA for your ASA and ASDM images.
  - Read Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

Configuration Prerequisites for Firepower 1000 and Firepower 2100 Series Devices

- The FXOS mode of a Firepower 2100 series device must be configured for **appliance** mode. See Set the Firepower 2100 to Appliance or Platform Mode for more information.
- The device must be running ASA Version 9.13(1) or later.
- You must upgrade the FXOS bundle prior to upgrading the ASA software. See Firepower 2100 ASA and FXOS Compatibility for more information.

Firepower 4100 and Firepower 9300 Series Devices Running ASA

CDO does not support the upgrade for the Firepower 4100 or Firepower 9300 series devices. You must upgrade these devices outside of CDO.

Upgrade Guidelines

- CDO can upgrade ASAs configured as an Active/Standby "failover" pair. CDO cannot upgrade ASAs configured in an Active/Active "clustered" pair.

Software and Hardware Prerequisites

Minimum ASA and ASDM versions from which you can upgrade:

- ASA: ASA 9.1.2
- ASDM: There is no minimum version.

Supported Hardware Versions

- See Devices, Software, and Hardware Supported by CDO.

Upgrade Bulk ASA and ASDM in CDO

Step 1 Review Prerequisites for ASA and ASDM Upgrade in CDO for upgrade requirements and important information about upgrading ASA and ASDM images.

Note If you are upgrading an ASA 1000 or 2000 series device, be sure to read Prerequisites for ASA and ASDM Upgrade in CDO.

Step 2 (Optional) In the navigation bar, click **Inventory**, create a Change Request Management to identify the devices upgraded by this action in the change log.

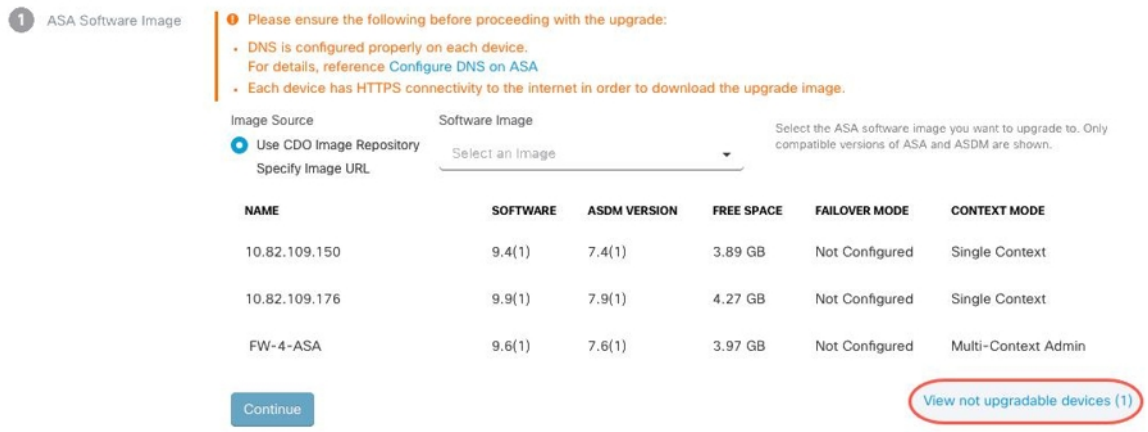
Step 3 Click the **Devices** tab.

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, CDO gives you a link to view the not upgradable devices.



Step 8 In step 1, click **Use** CDO **Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

The list indicates how many of the ASAs you chose can be upgraded to the software version you chose. In the example below, all of the devices can be upgraded to version 9.9(1.2), two devices can be upgraded to 9.8(2), and one of the devices can be upgraded to 9.6(1).

CDO alerts you if any of the software versions you chose are incompatible with any of the devices you chose. In the example below, CDO cannot upgrade the 10.82.109.176 device to a version earlier than it already runs.

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
✔ 10.82.109.150	9.4(1)	7.4(1)	3.89 GB	Not Configured	Single Context
✔ FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin
✖ 10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context

Step 9 In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.

Step 10 In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

Step 11 Click **Perform Upgrade** when you are ready.

Note If the upgrade fails, CDO displays a message. Often the reason for a failed upgrade is a network issue preventing the ASA and ASDM images from being transferred to the ASA.

Step 12 Alternatively, if you want CDO 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 13 (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade.

Step 14 Look at the Monitor Jobs in CDO 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 CDO.

Step 15 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.

Upgrade Multiple ASAs with Images from your own Repository

Step 1 Review Prerequisites for ASA and ASDM Upgrade in CDO for upgrade requirements and important information about upgrading ASA and ASDM images.

Step 2 (Optional) From the **Inventory** page, create a Change Request Management to identify the devices upgraded by this action in the change log.

Step 3 Click the **Devices** tab.

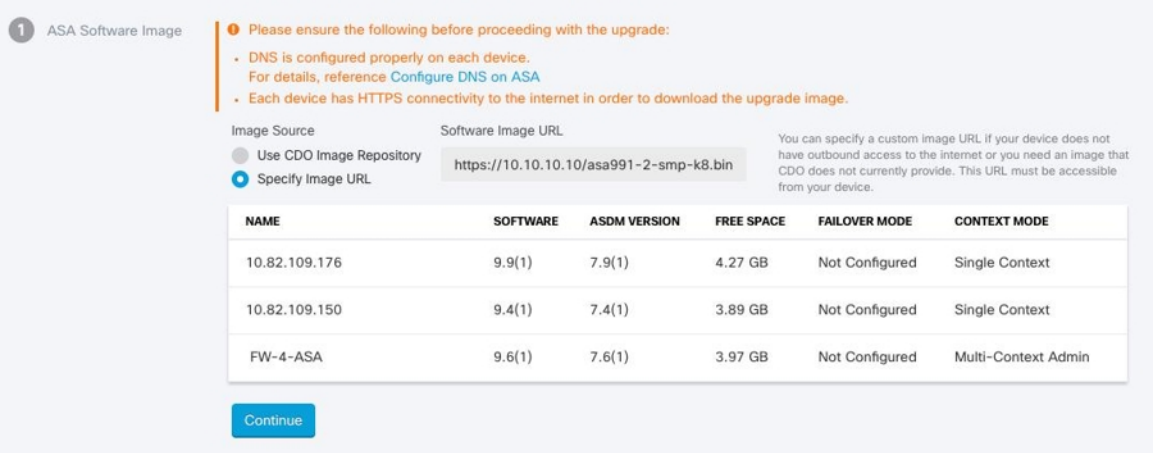
Step 4 Use the Filters, on page 88 to narrow down the list of devices you may want to include in your bulk upgrade.

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 In step 1, click **Specify Image URL,** enter the URL to the ASA image you want to upgrade to in the In the **Software Image URL** field, and click **Continue**. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

Note The picture below shows an HTTPS URL in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.



Step 8 In step 2, click **Specify Image URL,** enter the URL to the ASDM image you want to upgrade to in the In the **Software Image URL** field, and click **Continue**.

Step 9 In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

Step 10 Click **Perform Upgrade** when you are ready.

Note If the upgrade fails, CDO displays a message. Often the reason for a failed upgrade is a network issue preventing the ASA and ASDM images from being transferred to the ASA.

Step 11 Alternatively, if you want CDO 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 12 (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade.

Step 13 Look at the Monitor Jobs in CDO 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 CDO.

Step 14 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.

What to do next

Upgrade Notes

- You can also monitor the progress of the batch of upgrades by opening the **Inventory** page and viewing the Configuration Status column in the table.
- 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. CDO takes you to the Device Upgrade page for that device.

Upgrade ASA and ASDM Images on a Single ASA

Follow this procedure to upgrade the ASA and ASDM images on a single ASA.

Step 1 Review Prerequisites for ASA and ASDM Upgrade in CDO for upgrade requirements and important information about upgrading ASA and ASDM images.

Note If you are upgrading an ASA 1000 or 2000 series device, be sure to read Prerequisites for ASA and ASDM Upgrade in CDO.

Step 2 In the left pane, click **Inventory**.

Step 3 Click the **Devices** tab.

Step 4 (Optional) Create a Change Request Management to identify the device upgraded by this action in the change log.

Step 5 Select the device you want to upgrade.

Step 6 In the **Device Actions** pane, click **Upgrade**.

Step 7 On the Device Upgrade page, follow the instructions presented to you by the wizard.

a. In step 1, click **Use** CDO **Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

Note When upgrading your ASAs and ASDMs to images stored in your own repository, select **Specify Image URL** and enter the URL of the ASA or ASDM image in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

(Optional) If you want CDO 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 **Schedule Upgrade**.

b. In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.

c. In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

Step 8 Click **Perform Upgrade** when you are ready.

Step 9 (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade. Want to see a demo? Watch a screencast of this procedure!

What to do next

Upgrade Notes

- If you select an image to upgrade to, and you change your mind, check the **Skip Upgrade** check box associated with the software image. The image will not be copied to the device, nor will the device be upgraded with the image.
- In the **Perform Upgrade** step, if you choose only to copy the images to the ASA, you can return to the Device Upgrade page later and click "Upgrade Now" to perform the upgrade. After the copying task is complete, you will see the message "Ready to Upgrade" for that device on the **Inventory** page.
- You cannot take action on a device during the process of copying the image, installing it, and rebooting the device. Devices that are installing the image and then rebooting are shown as "Upgrading" in the **Inventory** page.
- You cannot take action on a device during the upgrade process; that is, installing the image and rebooting the device.
- You can take action on a device if you choose only to copy the images to the device. Devices that are copying images are shown as "Copying Images" in the **Inventory** page.
- Upgrading devices that have self-signed certificates may experience issues; see Troubleshoot New Certificate Issues for more information.

Upgrade ASA and ASDM Images in a High Availability Pair

Before you upgrade your pair of ASAs in active/standby failover mode, review the prerequisites below. If you need more information about how ASAs are configured and work in failover mode, see Failover for High Availability in the ASA documentation.

Want to see a demo? Watch a screencast of this procedure.

Prerequisites

- Review Prerequisites for ASA and ASDM Upgrade in CDO for requirements and important information about upgrading ASA and ASDM images.
- The primary (active) and secondary (standby) ASAs are configured in active/standby failover mode.
- The primary ASA is the active device in the active/standby pair. If the primary ASA is inactive, CDO will not perform the upgrade.
- The primary and secondary ASA software versions are the same.

Workflow

This is the process by which CDO upgrades the active/standby pair of ASAs:

Step 1 CDO downloads the ASA and ASDM images to both ASAs.

Note Users have the choice of downloading ASA and ASDM images but not upgrading immediately. If the ASA and ASDM images were downloaded previously, CDO will not download them again; CDO continues the upgrade workflow with the next step.

Step 2 CDO upgrades the secondary ASA first.

Step 3 Once the upgrade is complete and the secondary ASA returns to the "Standby-Ready" state, CDO initiates a failover so that the secondary ASA becomes the active ASA.

Step 4 CDO upgrades the primary ASA, which is now the current standby ASA.

Step 5 Once the primary ASA returns to the "Standby-Ready" state, CDO initiates a failover so that the primary ASA becomes the active ASA.

Warning Upgrading devices that have self-signed certificates may experience issues; see Troubleshoot New Certificate Issues for more information.

Upgrade ASA and ASDM Images in a High Availability Pair

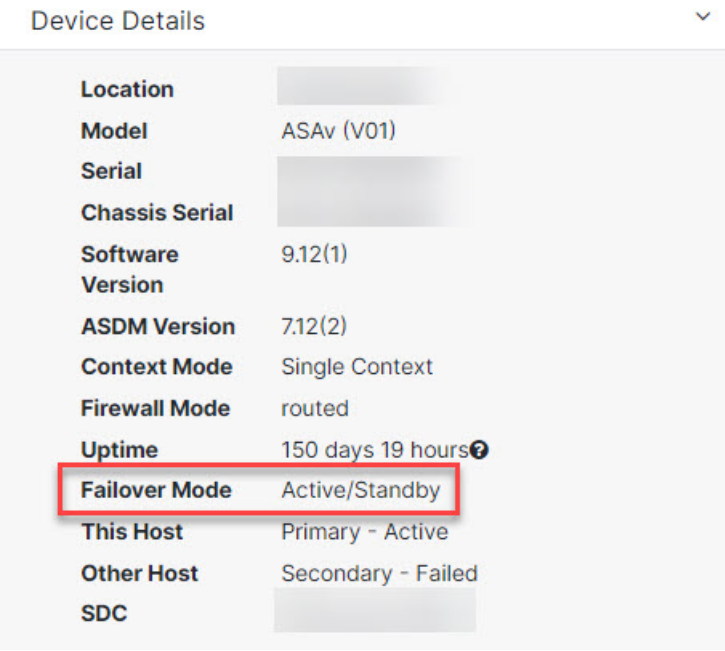
Step 1 In the left pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Select the device you want to upgrade.

Step 4 In the **Device Actions** pane, click **Upgrade**.

Notice that the failover mode of the device is Active/Standby:



Step 5 On the Device Upgrade page, follow the instructions presented to you by the wizard.

Note When upgrading your ASAs and ASDMs to images stored in your own repository, select **Specify Image URL** and enter the URL of the ASA or ASDM image in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

Upgrade an ASA or ASDM Using Your Own Image

When you upgrade your ASA with new ASA software and ASDM images, you can either use images that Cisco Defense Orchestrator stores in its image repository or you can use images that you store in your own image repository. If your ASA does not have outbound access to the internet, maintaining your own image repository is the best option for upgrading your ASAs using CDO.

CDO uses ASA's copy command to retrieve the image and copy it to the flash drive (disk0:/) of your ASA. In the Specify Image URL field you are providing the URL portion of the copy command. For example, if the whole copy command would have been:

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

You are providing:

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

in the Specify Image URL field.

CDO supports http, https, ftp, tftp, smb, and scp methods of retrieving the upgrade image.

URL Syntax examples

Here are examples of URL syntax for the ASA copy command. For the sake of these URL examples, assume the following:

- **Image repository address**: 10.10.10.10
- **Username to access the image repository**: admin
- **Password**: adminpass
- **Path**: images/asa
- **Image filename**: asa991-smp-k8.bin

http[**s**]**://** [[*user* [: *password*] **@**] *server* [: *port*] **/** [*path* **/**] *filename*]

https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin

ftp:// [[*user* [: *password*] **@**] *server* [: *port*] **/** [*path* **/**] *filename* [**;type=** *xx*]]â€"The **type** can be one of these keywords: **ap** (ASCII passive mode),**an** (ASCII normal mode), **ip**(Defaultâ€"Binary passive mode), **in** (Binary normal mode).

ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin

tftp:// [[*user* [: *password*] **@**] *server* [: *port*] **/** [*path* **/**] *filename* [**;int=** *interface_name*]]

tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside

Note The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command. The **;int=** *interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server.

smb:/[[*path* **/**] *filename*] - Indicates a UNIX server local file system.

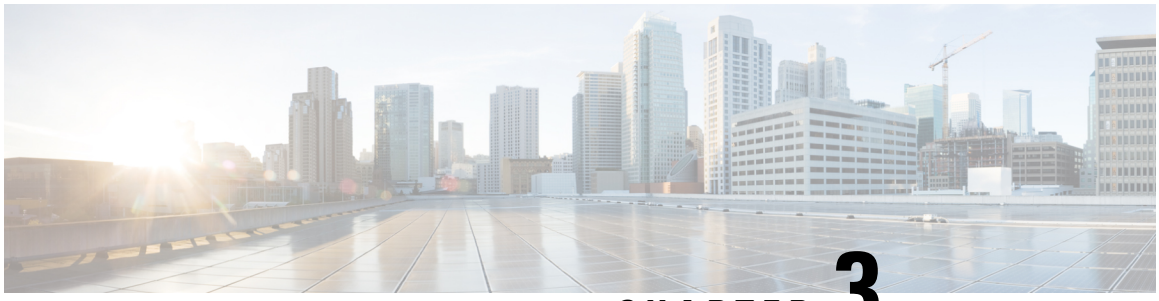
smb:/images/asa/asa991-smp-k8.bin

scp:// [[*user* [: *password*] **@**] *server* [**/** *path*] **/** *filename* [**;int=** *interface_name*]]â€"The**;int=** *interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.

scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
SCP example without a username and password:
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside

The complete copy command with URL syntax in the Cisco ASA Series Command Reference, A - H Commands guide.

See Prerequisites for ASA and ASDM Upgrade in CDO for more information about upgrading ASA and ASDM images using a custom URL.



CHAPTER 3

Configuring ASA Devices

This chapter covers the following sections:

Update ASA Connection Credentials in CDO

In the process of onboarding an ASA, you entered the username and password CDO must use to connect to the device. If those credentials are changed on the device, use the **Update Credentials** device action to update those credentials on CDO as well. This feature allows you to update the credentials on CDO without having to re-onboard the device. The username and password combination you switch to must already exist on the ASA or Authentication, Authorization, and Accounting (AAA) server for that user. This process only affects the Cisco Defense Orchestrator database; no changes to the ASA configuration are made when using the Update Credentials feature.

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

Step 2 Click the **Devices** tab and then click **ASA**.

Step 3 Select the ASAs whose connection credentials it is you want to update. You can update the credentials on one or multiple ASAs at once.

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

Step 5 Select the Cloud Connector or the Secure Device Connector (SDC) you use to connect the ASA(s) to CDO.

Step 6 Enter the new username and password you want to use to connect to the ASAs.

Step 7 After the credentials are changed, CDO syncs the device.

Note If CDO fails to sync the device, the connectivity status in CDO may show "Invalid Credentials." If that's the case, you may have tried to use an invalid username and password combination. Make sure the credentials you want to use are stored on your ASA or AAA server, and try again.

Move an ASA from one SDC to Another

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

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

Step 2 Select the ASAs you want to move to the other SDC.

Step 3 In the Device Actions pane, click **Update Credentials**.

Step 4 Click the Secure Device Connector button and select the SDC you want to move the device to.

Step 5 Enter the administrator username and password you used to onboard the ASA, and click Update. You do not have to deploy these changes to the device.

ASA Interface Configuration

Cisco Defense Orchestrator (CDO) simplifies ASA interface configuration by providing a user-friendly interface that eliminates the need to use the command line interface. You have complete control over configuring the ASA's physical interfaces, subinterfaces, and EtherChannels. Moreover, you can also view Virtual Tunnel Interfaces that are created during route-based site-to-site VPN, but they are read-only. You can use CDO to configure and edit data interfaces or the management/diagnostic interface on an ASA device.

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.

Management Interface

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management Slot/Port interface (if available for your model)

Use MTU Settings

The MTU specifies the maximum frame payload size that the 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.

Read-only Support for Virtual Tunnel Interface (VTI)

Configuring a route based site-to-site VPN tunnel between two ASA devices creates a Virtual Tunnel Interface (VTI) between the devices. Devices with configured VTI tunnels can be onboarded to CDO, which discovers and lists them on the **ASA Interfaces** page but doesn't support their management.

Configure an ASA Physical Interface

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 Click a physical interface that you want to configure, and click **Edit**.

The **Editing Physical Interface** dialog box appears.

Step 5 In the **Logical Name** field, enter a name for the interface.

Step 6 Continue with one of the following procedures:

- Configure IPv4 Addressing for ASA Physical Interface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Physical Interface, on page 147 if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. 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 ASA Physical Interface.

Configure IPv4 Addressing for ASA Physical Interface

Step 1 In the **Edit Physical Interface** dialog box, configure the following in the **IPv4 Address** tab:

- **Type**: You can use either static IP addressing or DHCP for the interface.

  Static - Choose this option if you want to assign an address that should not change.

  - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
  - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

    For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

  DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

  You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

Step 2 Click **Save** if you are done or continue with one of these procedures.

- Configure IPv6 Addressing for ASA Physical Interface, on page 147 if you intend to assign an IPv6 address to this interface.

- Configure Advanced ASA Physical Interface Options. 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 ASA Physical Interface.

Configure IPv6 Addressing for ASA Physical Interface

Step 1 In the **Editing Physical Interface** dialog box, click the **IPv6 Address** tab.

Step 2 Configure the following:

- **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.

- **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 device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Suppress RA**: Check this box if you want to suppress router advertisements. The 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 device to supply the IPv6 prefix (for example, the outside interface).

- **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.
- **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.

- **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 device, to which this interface is connected.
- **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. You can add another static address.
- **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 3 Click **Save** if you are done or continue with one of these procedures.

- Configure Advanced ASA Physical Interface Options. 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 ASA Physical Interface.

Configure Advanced ASA Physical 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.

Step 1 In the **Editing Physical Interface** dialog box, click the **Advanced** tab.

Step 2 Configure the following advanced settings:

- **HA Monitoring**: Enable to include 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.
- **Management Only**: Enable 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 a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **Duplex and Speed (Mbps)**: 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 Limitations for Interface Configuration.

- **Duplex**: Choose Auto, Half, or Full. Auto is the default when the interface supports it.
- **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:

- **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.
- **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 3 If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the ASA Physical Interface.

Step 4 Click **Save**.

Enable the ASA Physical Interface

Step 1 Select the physical interface you want to enable.

Step 2 Move the **State** slider at the top right of the window associated with the interface's logical name.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made.

Add an ASA VLAN Subinterface

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.

- Configure ASA VLAN Subinterfaces

Configure IPv4 Addressing for ASA Subinterface, on page 150

- Configure IPv6 Addressing for ASA Subinterface, on page 151
- Configure Advanced ASA Subinterface Options, on page 152
- Enable the Subinterface, on page 153

Configure ASA VLAN Subinterfaces

Step 1 In the CDO navigation pane, click **Inventory**.

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 You can add a subinterface using one of the following methods:

- Choose  > **Subinterface**
- Click a physical interface that you want to configure and in the **Actions** pane on the right, click **New Subinterface**.

Step 5 In the **VLAN ID** field, enter the VLAN ID between 1 and 4094.

Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.

Step 6 In the **Subinterface ID** field, enter the subinterface ID as an integer between 1 and 4294967293.

The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.

Step 7 Continue with one of the following procedures:

- Configure IPv4 Addressing for ASA Subinterface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Subinterface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Subinterface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure IPv4 Addressing for ASA Subinterface

Step 1 In the **Creating Subinterface** dialog box, configure the following in the **IPv4 Address** tab:

- **Type**: You can use either static IP addressing or DHCP for the interface.

  Static - Choose this option if you want to assign an address that should not change.

  - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
  - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

Step 2 Click **Save** if you are done or continue with one of these procedures.

- Configure IPv6 Addressing for ASA Subinterface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Subinterface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the ASA Physical Interface.

Configure IPv6 Addressing for ASA Subinterface

Step 1 In the **Creating Subinterface** dialog box, click the **IPv6 Address** tab.

Step 2 Configure the following:

- **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.

- **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 device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Suppress RA**: Check this box if you want to suppress router advertisements. The 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 device to supply the IPv6 prefix (for example, the outside interface).

- **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.
- **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.

- **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 device, to which this interface is connected.
- **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. You can add another static address.
- **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 3 Click **Save** if you are done or continue with one of these procedures.

- Configure Advanced ASA Subinterface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure Advanced ASA Subinterface 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.

Step 1 In the **Creating Subinterface** dialog box, click the **Advanced** tab.

Step 2 Configure the following advanced settings:

- **HA Monitoring**: Enable to include 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.
- **Management Only**: Enable 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 a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **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.
- **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 3 If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Subinterface.

Step 4 Click **Save**.

Enable the Subinterface

Step 1 Select the subinterface you want to enable.

Step 2 Move the **State** slider at the top right of the window associated with the interface's logical name.

Step 3 Review and deploy the changes you made.

Remove ASA Subinterface

Use the following procedure to remove an subinterface from ASA.

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 On the **Interfaces** page, expand the physical interface linked with the subinterface you want to delete and then select that specific subinterface.

Step 5 In the **Actions** pane located to the right, click **Remove**.

Step 6 Confirm you want to delete the EtherChannel interface and click **Delete**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made.

About ASA EtherChannel Interfaces

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

See the **EtherChannel and Redundant Interfaces** chapter of ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X, Y for more information on ASA EtherChannel interfaces.

Configure ASA EtherChannel

Use this procedure to add a new EtherChannel interface to an ASA.

Before you begin

To configure EtherChannel on ASA interface, the following prerequisites must be met:

- 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, except for the Secure Firewall 3100, which supports different interface capacities as long as the speed is set to Detect SFP; in this case, the lowest common speed is used.
- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name.
- You cannot add an interface part of another EtherChannel interface group, Switchport interfaces, and interfaces with subinterfaces.

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 Choose  > **EtherChannel Interface**.

Step 5 In the **Logical Name** field, provide a name for the EtherChannel interface.

Step 6 In the **EtherChannel ID**, enter an integer between 1 and 8.

Step 7 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 8 Search for and select the interfaces you want to include in the EtherChannel as members. 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, CDO removes the IP address of the member.

Step 9 Select the **IPv4**, **IPv6**, or **Advanced** tab to configure the IP address of the subinterface.

- Configure IPv4 Addressing for ASA Physical Interface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Physical Interface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 10 Move the **State** slider at the top right of the window to enable the EtherChannel interface.

Step 11 Click **Save**.

Step 12 Preview and Deploy Configuration Changes for All Devices the changes you made.

Edit ASA EtherChannel

Use this procedure to edit an existing EtherChannel on ASA.

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 On the **Interfaces** page, select the EtherChannel interface you want to edit.

Step 5 In the **Actions** pane located to the right, click **Edit**.

Step 6 Modify the values you want and click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made.

Remove ASA EtherChannel Interface

Use the following procedure to remove an EtherChannel interface from ASA.

Step 1 In the left pane, click **Inventory**.
Step 2 Click the **ASA** tab.
Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
Step 4 On the **Interfaces** page, select the EtherChannel interface you want to delete.
Step 5 In the **Actions** pane located to the right, click **Remove**.
Step 6 Confirm you want to delete the EtherChannel interface and click **Delete**.
Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made.

ASA System Settings Policy in CDO

Introduction to ASA System Settings Policy

Manage your ASA device's operations and functionalities using a System Settings policy. This policy includes essential configurations like domain name services, enabling the secure copy server, message logging, and permitting VPN traffic without checking ACLs. By setting up a policy, you can ensure that your device is properly configured to maintain a secure network environment.

When configuring an ASA device, it's important to note that you have the option to manage multiple devices' settings with a shared system settings policy, or you can individually edit the settings for any single device.

Shared System Settings Policy

A shared system settings policy applies to multiple ASA devices in your network. It makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes made to a parameter of a shared policy affect the other ASA devices that use the policy.

Choose **Policies** > **ASA System Settings**. See Create an ASA Shared System Settings Policy, on page 156.

You can also modify the device-specific system settings specific to a single ASA device to override the shared system settings policy values. Choose **Inventory** > **ASA device** > **Management** > **Settings**. See Configure or Modify Device Specific System Settings, on page 163.

Create an ASA Shared System Settings Policy

Use this section to create a new shared system settings policy for ASA devices.

Step 1 Choose **Policies** > **ASA System Settings**.
Step 2 Click  .
Step 3 In the **Name** field, enter a name for the policy and click **Save**.
Step 4 In the edit ASA shared system settings page, configure the parameters you want:

- Configure Basic DNS Settings, on page 157

- Configure HTTP Settings, on page 158
- Set the Date and Time Using an NTP Server, on page 158
- Configure SSH Access, on page 159
- Configure System Logging, on page 160
- Enable Sysopt Settings, on page 162

Note

- An orange dot ( ) on the corresponding parameter highlights unsaved changes.
- The denied symbol ( ) highlights parameters that use existing local values from the device.

Configure Basic DNS Settings

You need to configure a DNS server so that the ASA can resolve host names to IP addresses. You also must configure a DNS server to use fully qualified domain names (FQDN) network objects in access rules.

Step 1 In the edit ASA system settings page, click **DNS** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. CDO uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 In the **DNS** section, click + to configure servers.

- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify DNS server's IP address.
- **Interface Name**: Specify the interface where the DNS lookup should be enabled.

Note Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

Step 4 Click **Save**.

Step 5 In the **Domain name** field, specify the domain name for the ASA.

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

Step 6 In the **DNS Lookup** section, click + and specify the interface name.

If you do not enable DNS lookup on an interface, then the ASA will not communicate with the DNS server on that interface. Make sure to enable DNS lookup on all interfaces that will be used to access DNS servers.

Note To remove a configured interface, you can click the delete icon under **Actions**.

Step 7 Click **Save**.

Configure HTTP Settings

To access the ASA interface for management access, you must specify the addresses of all hosts/networks which are allowed to access the ASA using HTTP. If you configure HTTP redirect to redirect HTTP connections to HTTPS automatically, you must enable an access rule to allow HTTP; otherwise, the interface cannot listen to the HTTP port.

Step 1 In the edit ASA system settings page, click **HTTP** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. CDO uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Check the **Enable HTTP Server** check box to enable the HTTP server.

Step 4 In the **Port Number** field, set the port number. The port identifies the port from which the interface redirects HTTP connections.

Warning If you change the HTTP port on your device, it may cause some problems with its connection to CDO. It's important to remember this if you plan to alter any settings related to your device's network connection.

Step 5 Click  to add HTTP information.

- **Interface**: Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using HTTP.
- **Netmask**: Specify the subnet mask for the network.

Note To remove a host, you can click the delete icon under **Actions**.

Step 6 Click **Save**.

Set the Date and Time Using an NTP Server

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is.

Time derived from an NTP server overrides any time set manually.

The ASA supports NTPv4.

Step 1 In the edit ASA system settings page, click **NTP** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. CDO uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Click  to add NTP server details.

- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the NTP server's IP address.

  You cannot enter a hostname for the server; the ASA does not support DNS lookup for the NTP server.
- **Key Id**: Enter a number between 1 and 4294967295.

  This setting specifies the key ID for this authentication key, which enables you to use authentication to communicate with the NTP server. The NTP server packets must also use this key ID.
- **Interface Name**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

  NTP uses an algorithm to determine which server is the most accurate and synchronizes to it. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one.
- **Prefer**: (optional) Check the **Preferred** check box to set this server as a preferred server.

Note To remove an NTP server, you can click the delete icon under **Actions**.

Step 4 Click **Save**.

Configure SSH Access

You can enable the secure copy (SCP) server on the ASA. Only clients that are allowed to access the ASA using SSH can establish a secure copy connection.

Step 1 In the edit ASA settings policy page, click **SSH** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. CDO uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Enable **Enable Scopy SSH** (secure copy SSH).

Step 4 In the **Timeout in Minutes** field, set the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases, and should be increased until all pre-production testing and troubleshooting have been completed.

Step 5 Click  and configure the following:

- **Interface**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using SSH.
- **Netmask**: Specify the subnet mask for the network.

Note To remove SSH details, you can click the delete icon under **Actions**.

Step 6 Click **Save**.

Configure System Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

Security Levels

The following table lists the syslog message severity levels.

Table 14: Syslog Message Severity Levels

Level Number	Security 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.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only. Log at this level only temporarily, when debugging issues. This log level can potentially generate so many messages that system performance can be affected.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

Step 1 In the edit ASA system settings page, click **Syslog** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. CDO uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Configure the following:

- **Logging Enabled**: Enable secure logging.
- **Timestamp Enabled**: Enable to include the date and time in syslog messages.
- **Permit host down**: (Optional) Disable the feature to block new connections when a TCP-connected syslog server is down.
- **Buffer Size**: Specify the size of the internal log buffer. The allowed range is 4096 to 1048576 bytes.
- **Buffered Logging Level**: Specify which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location.
- **Console Logging Level**: Specify which syslog messages should be sent to the console port.
- **Trap Logging Level**: Specify which syslog messages should be sent to the syslog server.

Step 4 Click + to add Syslog server details.

- **Interface Name**: Specify the interface name on which the syslog server resides. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the IP address of the syslog server.
- **Protocol**: Choose the protocol (**TCP** or **UDP**) the ASA should use to send syslog messages to the syslog server.
  - **Port**: Specify the port that the syslog server listens to for syslog messages. The allowed TCP port range is 1 to 65535, and the UDP port range is 1025 to 65535.
  - **Log messages in Cisco EMBLEM format (UDP only)**: Enables EMBLEM format logging for the syslog server with UDP only.
  - **Enable secure syslog using SSL?**: Specifies that the connection to the remote logging host should use SSL/TLS for TCP only.
- **Reference Identity**: Specify the reference identity type to enable RFC 6125 reference identity checks on the certificate based on the previously configured reference identity object. See Configure Reference Identities for details on the reference identity object.

Note To remove a Syslog server, you can click the delete icon under **Actions**.

Step 5 Click **Save**.

Enable Sysopt Settings

The crypto map ACL bound to the outgoing interface either permits or denies IPsec packets through the VPN tunnel. IPsec authenticates and deciphers packets that arrive from an IPsec tunnel, and subjects them to evaluation against the ACL associated with the tunnel.

ACLs define which IP traffic to protect. For example, you can create ACLs to protect all IP traffic between two subnets or two hosts.

Step 1 In the edit ASA system settings page, click **Sysopt** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. CDO uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Enable **Allow VPN traffic to bypass interface access lists** bypasses the ACL inspection.

Step 4 Click **Save**.

Assign a Policy from the Shared System Settings Page

After configuring a shared system settings policy, assign onboarded ASA devices and deploy the settings to the devices for the changes to take effect. Any change made to the policy affects the devices that are associated with the policy.

You can also Assign a Policy from Device-Specific Settings Page page.

Note You can associate an ASA device to only one shared system settings policy.

Step 1 Choose **Policies** > **ASA System Settings**.

Step 2 Select a shared policy and click **Edit**.

Step 3 Click the filter appearing beside the policy name to assign devices.

Step 4 Select the ASA devices you want to associate with the selected policy and click **OK**.

Note The checkboxes are ticked for devices that are already associated with the selected policy.

If you see a red icon , it means that an error has occurred while applying the shared system settings policy to your devices. To troubleshoot the issue, click the policy on the **ASA System Settings** page and in the **Error Detected** pane, click the **Device Workflows** to get more information.

Step 5 Deploy Configuration Changes Made Using the CDO GUI the changes you have made.

Configure or Modify Device Specific System Settings

A device-specific system settings are existing values specific to an ASA device that can be modified using CDO. You can override the shared system settings policy values with existing device-specific values for parameters you want.

This topic describes configuring an onboarded ASA device's system settings.

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

Step 2 Click the **ASA** tab.

Step 3 Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

You will see the device-specific system settings of the selected ASA device.

Note If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. You can also assign a policy from the device-specific settings page. Select the ASA devices you want to associate with the selected policy and click **OK**

Step 4 Configure or modify the values of the system settings you want and click **Save**.

Note The field descriptions for a shared and device-specific system settings remain the same. You can click the corresponding link below for more information.

- Configure Basic DNS Settings, on page 157
- Configure HTTP Settings, on page 158
- Set the Date and Time Using an NTP Server, on page 158
- Configure SSH Access, on page 159
- Configure System Logging, on page 160
- Enable Sysopt Settings, on page 162

You can click **Return to Inventory** to navigate to the inventory page.

Step 5 Click **Save** after making the changes.

Note An orange dot ( ) on the corresponding parameter highlights unsaved changes.

Assign a Policy from Device-Specific Settings Page

You can also assign a policy from the device-specific settings page of an onboarded ASA device.

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

Step 2 Click the **ASA** tab.

Step 3 Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

You will see the device-specific settings of the selected ASA device.

Note If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. Select the ASA devices you want to associate with the selected policy and click **OK**

Step 4 Click the **Parent Policy** button to assign a shared system settings policy.

Step 5 Select a policy and click **Apply**.

Step 6 Deploy Configuration Changes Made Using the CDO GUI the changes you have made.

Auto Assignment of ASA Devices to a Shared System Settings Policy

When onboarding a new ASA device, or checking for changes or handing out-of-band changes for existing devices, CDO verifies whether:

- The device-specific settings match a pre-existing shared system settings policy. If there is a match, the device gets assigned to the shared system settings policy.
- The device-specific settings of the onboarded devices match each other. If they do, a new shared system settings policy gets created automatically, and devices with the same local settings are assigned to this shared policy.

Note You can rename the Shared Settings policy whether it was created by the user or the system.

Filter ASA Shared System Settings Policy

If you're searching for specific shared system settings policies on the ASA System Setting page, you can use filters based on issues and usage to narrow down your search and find what you're looking for more easily.

Choose **Policies** > **ASA System Settings** > .

- **Issues**:
  - **Issue Detected**: Displays only the policies that have issues when applying devices to them.
  - **No issue**: Displays only the policies that are successfully applied to devices.
- **Usage**:
  - **In Use**: Displays policies that have are assigned to devices.
  - **Unused**: Displays policies that have not been assigned to any devices yet.

Disassociate Devices from Shared System Settings Policy

If an ASA device is no longer needed in the shared system settings policy, you can easily dissociate it. The device detaches from the policy when:

- Changes are made to the device-specific settings, where the corresponding setting on the shared policy is not configured to retain existing values from the device.
- Devices are detached manually from the shared system settings policy.
- Shared system settings policy is deleted from CDO. However, this doesn't delete the device. See Delete Shared Settings Policy, on page 165.

Step 1 Choose **Policies** > **ASA System Settings**.

Step 2 Select a shared policy and click **Edit**.

Step 3 Click the filter appearing beside the policy name to detach devices.

Step 4 Uncheck the devices you want to detach from the selected shared system settings policy and click **OK**.

Note The changes are saved automatically and don't require any manual deployment.

Delete Shared Settings Policy

If you want to remove some shared settings policies, you have the option to select one or more of them and delete them. However, it's important to note that you can only delete them if they haven't been applied or committed to any devices yet.

Before you begin

Ensure the devices are dissociated from the shared settings policy you wish to delete. See Disassociate Devices from Shared System Settings Policy for more information.

Step 1 In the left pane, choose **Policies** > **ASA System Settings**.

Step 2 Select a shared policy and click **Delete**.

Step 3 Click **OK** to confirm your action.

Note If you delete an ASA from CDO, the device-specific settings and configurations will also be deleted, and the device references will be removed from the shared settings policy.

ASA Routing in CDO

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth that is used by routing algorithms to determine the optimal path to

a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which include route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with various information. Destination or next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables can also include other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of various messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message that is sent between routers, informs other routers of the state of the sender links. Link information can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

About ASA Static Route

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

For general information on how ASA routing concepts and CLI commands, see the following documents:

- *Static and Default Routes* chapter from ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X,Y.
- *Static and Default Routes* chapter from CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, X,Y.

Default Route

The simplest option is to configure a default static route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the ASA sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

You should always define a default route.

Static Route

You might want to use static routes in the following cases:

- Your networks use an unsupported router discovery protocol.
- Your network is small and you can easily manage static routes.
- 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 ASA.

- You are using a feature that does not support dynamic routing protocols.

Static Route Tracking

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The ASA implements static route tracking by associating a static route with a monitoring target host on the destination network that the ASA monitors using ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address.
- The next hop gateway address (if you are concerned about the availability of the gateway).
- A server on the target network, such as a syslog server, that the ASA needs to communicate with.
- A persistent network object on the destination network.

Configure ASA Static Route

A static route defines where to send traffic for specific destination networks.

This section describes the steps to add a static route to an ASA device.

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

Step 2 Click the **ASA** tab.

Step 3 Select a device you want to configure a static route.

Step 4 In the **Management** pane on the right, click **Routing**.

Step 5 Click  to add a static route.

Step 6 You can enter a **Description** for the route.

Step 7 Select whether the route is for an **IPv4** or **IPv6** address.

Step 8 Configure the route properties:

- **Interface**: Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.

  You can use a **Null0** route to forward unwanted or undesirable traffic so the traffic is dropped. Static Null0 routes have a favorable performance profile. You can also use static null0 routes to prevent routing loops.

  The ASA CLI accepts both Null0 or null0 strings.
- **Gateway IP**: (Not applicable to a **Null0** route) 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 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 IP**: Select the network object(s), that identifies the destination network, that contains the host(s), that uses the gateway in this route.
- **Destination Mask** (only for IPv4 addressing): Enter the subnet mask for the destination IP.
- **Tracking** (only for IPv4 addressing): Enter a unique identifier for the route tracking process.

Step 9 Click **Save**.

Step 10 Deploy Configuration Changes Made Using the CDO GUI the changes you made, or wait and deploy multiple changes at once.

Edit ASA Static Route

You can edit the static route parameters associated with an ASA device.

Note However, you cannot select a different IP version while modifying the static route. Alternatively, you can create a new static route based on your requirement.

Step 1 Select an ASA device you want to edit the static route.

Step 2 In the **Management** pane on the right, click **Routing**.

Step 3 In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Edit**.

Step 4 Modify the values you want and click **Save**. See Configure ASA Static Route, on page 167 for information on the routing parameters.

Step 5 Deploy Configuration Changes Made Using the CDO GUI the changes you made, or wait and deploy multiple changes at once.

Delete a Static Route

Before you begin

Deleting a static route may impact the connectivity to your device's local SDC or CDO. Ensure a proper disaster recovery procedure is in place for any connectivity loss.

Step 1 Select an ASA device you want to delete.

Step 2 In the **Management** pane on the right, click **Routing**.

Step 3 In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Delete**.

Step 4 Click OK to confirm the changes.

Step 5 Deploy Configuration Changes Made Using the CDO GUI the changes you made, or wait and deploy multiple changes at once.

Manage Security Policies in CDO

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 CDO to configure security policies on many different types of devices.

- Create an ASA Access List
- Network Address Translation, on page 183

Manage ASA Network Security Policy

The ASA network security policy includes access control lists (ACLs) that determine whether to permit or deny traffic from accessing another network through the ASA firewall. This section outlines the steps to create an ASA access list and configure access rules within it. It also details the steps to assign an interface to an access control list and share it among other ASA devices managed by CDO.

About ASA Access Control Lists and Access Groups

ASA Access Control Lists

Access control lists (ACLs) are used to identify traffic flows based on various characteristics such as source and destination IP address, IP protocol, ports, source, and other parameters.

The following is an access list sample:

```
access-list ACL extended permit ip any any
```

`ACL` is the name of the access list.

You can avoid the creation of the same access list on multiple devices individually, and instead create a single access list and share it across multiple ASA devices. Changes made to the shared access list automatically apply to all the devices to which the ACL is assigned. You also have the option to copy the access list to other ASA devices as needed.

Access Rules

An access list includes access rules that permit or deny traffic flow to a network based on specific characteristics such as source and destination IP addresses, IP protocol, port number, and security group tags.

ASA Access Groups

An access group is a specific association that is established when an access list is assigned to a device interface configured for traffic flow in any direction. The access list contains specific rules that either permit or deny traffic passing through the device interface.

The following is an access group sample that is created when a device interface is assigned to an access list.

```
access-group ACL out interface giginterface0
```

`ACL` is the name of the access list and `giginterface0` is the logical name of the device interface that is assigned to the access list.

Note To use API endpoints to manage your ASA access groups, see Get Access Groups on the Cisco DevNet website.

Create an ASA Access List

When configuring an access list on an ASA firewall, a rule is automatically created to allow traffic from a source to a destination outside your network. You can create additional rules and assign the access list to an interface to regulate the traffic network.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 Click **Create Access List**.

Step 5 In the **Name** field, enter a name for the access list and click **Save**.

Note You cannot have two access lists with the same name on a device.

Step 6 Click **Save**.

CDO creates an access group and a default rule that permits all traffic.

You can now add new rules to the access list. See Add a Rule to an ASA Access List, on page 170.

What to do next

- To add new rules to the access list, see Add a Rule to an ASA Access List, on page 170.
- To assign interfaces and traffic directions to the access list, see Assign Interfaces to ASA Access Control List, on page 173.

Add a Rule to an ASA Access List

You can add rules in ascending order by rule number. Packets will be verified against the rules in the sequence in which the rules were created, with the first rule taking precedence, followed by subsequent rules. You can adjust the position of any rule, if required.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, select an access list that you want.

Step 5 Click the **Add Rule** ( ) icon that is displayed on the right.

Note In the ordered list, hover over the desired position and click **Add Rule Here**.

Step 6 In the **New Access Rule** window, provide the following information:

- **Order**: Select where you want to insert the rule in the ordered list of rules. Rules are applied on a first-match basis and prioritized by position in the list of rules from 1 to last.
- **Action**: Specify whether you are allowing (permitting) the described traffic or are blocking (dropping) it.
- **Protocol**: Specify the protocol of the traffic, such as IP, TCP, UDP, ICMP, or ICMPv6. The default is IP, but you can select a more specific protocol to target traffic with more granularity.
- **Source/Destination**: Define the source (originating address) and destination (target address of the traffic flow). You typically configure the IPv4 address of hosts or subnets, which you can represent with network object groups. You can assign only one object to the source or destination. To create a new network object or group, see Create or Edit ASA Network Objects and Network Groups.
- **Port**: Select the port object that pairs a service type, such as TCP or UDP, and a port number or a range of port numbers.
- **SGT Group**: Assign the security group you want from the list. By default, the value is **Any**. See About Security Group Tags in ASA Policies.
- **Time Range**: Define a time range for ASA network policies to allow access to networks and resources based on time of day. See ASA Time Range Objects.
- **Logging**: Activity resulting from a network policy rule is not logged by default. You can activate logging for individual rules. See About System Log Activity .

Step 7 Click **Save**.

The rule is added to the access list and set to **Active** state.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

About System Log Activity

When you set up a new rule, you can specify how often and at what severity level you want to collect its activity. To do this, you can select the corresponding severity levels and then choose the frequency of data collection. This will ensure that you have the necessary information to monitor and analyze the activity generated by your rules.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

You have the option to adjust the logging interval, which indicates how frequently the log records are updated. This interval is measured in seconds and can be set from 1 to 600. By default, the interval is set to 300 seconds.

This interval value is also utilized as a timeout period for removing an inactive flow from the cache that collects drop statistics.

Table 15: Log Rule Activity

Security Level	Description
emergencies	System is unusable.
alert	Immediate action is needed.
critical	Critical conditions.
error	Error conditions.
warning	Warning conditions.
notification	Normal but significant conditions.
informational	Informational messages only.
debugging	Debugging messages only.

Deactivate Rules in an Access Control List

When you create a new rule in an access control list, it is activated by default. However, you can temporarily deactivate individual rules to optimize traffic flow, resolve conflicts, or isolate issues.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose the access control list you want.

Step 5 In the rule list, check the corresponding rule check box that you want.

Step 6 In the selected row, slide the **Active** setting off.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

About Security Group Tags in ASA Policies

If you onboard an ASA that uses security group tags (SGT) in its access control rules, Cisco Defense Orchestratorallows you to edit the rules that use SGT groups and manage the policies that have these rules. However, you cannot create SGT groups or edit them using the CDO GUI. To create or edit SGT groups, you must use ASA's Adaptive Security Device Manager (ASDM) or the CLI available in CDO.

In CDO's object page, when looking at the details of SGT groups, you'll see that those objects are identified as noneditable, system-provided objects.

CDO administrators can perform these tasks on ACLs and ASA policies that contain SGT groups:

- Edit all aspects of ACLs except the source and destination security groups.

- Copy a policy containing SGT groups from one ASA to another.

For detailed instruction, on configuring Cisco TrustSec using the command line interface, see the "ASA and Cisco TrustSec" chapter of the ASA CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide pertaining to your ASA release.

Assign Interfaces to ASA Access Control List

When you assign ASA interfaces to access control list, the device establishes a specific association between the list and interfaces. The rules that are associated with access control list are applied only to the interfaces through which the traffic flows in the specified directions.

You can only assign one access list per interface for a single traffic flow direction.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane displayed on the right, click **Assign Interfaces**.

Step 6 From the **Interface** drop-down list, choose an interface.

Step 7 From the **Direction** drop-down list, specify the direction for applying the selected access list.

The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

To apply the access list to all the interfaces on the ASA device, see Create an ASA Global Access List, on page 173.

Step 8 Click **Save**.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Create an ASA Global Access List

Global access policies are network policies that are applied to all the interfaces on an ASA. These policies are only applied to inbound network traffic. You can create a global access policy to ensure that a set of rules is applied uniformly to all the interfaces on an ASA.

Only one global access policy can be configured on an ASA. However, a global access policy can have more than one rule assigned to it, just like any other policy.

This is the order of rule-processing on the ASA:

1. Interface access rules
2. Bridge Virtual Interface (BVI) access rules
3. Global access rules
4. Implicit deny rules

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane displayed on the right, click **Assign Interfaces**.

Step 6 Check the **Create as a global access list** check box.

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.

Share an ASA Access Control List with Multiple ASA Devices

Sharing access policies in network security effectively improves efficiency, consistency, and centralized management, leading to an overall improved security posture. With a shared access control list, you can define access rules once on an ASA device and apply them to other CDO-managed ASA devices rather than configuring them separately. This ensures consistency in the network and reduces the risk of misconfigurations. Additionally, shared access control lists provide scalability because networks grow and evolve by allowing you to manage access control lists for increasing users and ASA devices.

Keep the following points in mind:

- Access control list rules are shared, but the interfaces are not included.
- Sharing an access control list with other ASA devices will overwrite any existing access control lists with the same name.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access control list.

Step 5 In the **Actions** pane that is displayed on the right, click **Share**.

Step 6 Select the ASA devices by checking the corresponding check box and click **Save**.

In the **Device Relationships** pane displayed on the right, the ASA devices that share the selected access control list are displayed.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Copy an ASA Access Control List to Another ASA

An ASA access control list can be easily copied to another CDO-managed device in the same tenant. After copying an access list file to a target ASA device, any further changes made to the access list won't be

automatically applied to the target device. This is different from access control list sharing feature, where changes are automatically applied.

Keep the following points in mind:

- You cannot copy an access list to a target device if that device already has another access list with the same name.
- You cannot copy an access list if another access list on the target device is associated with the same interface and direction.
- You cannot only copy an access list to a disabled interface on the target device.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane on the right, click **Copy**.

Step 6 Select the target device to which you want to copy the access list.

Step 7 Choose an interface and specify the direction for applying the selected access list.

The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

To apply the access list to all the interfaces on the selected target, see Create an ASA Global Access List, on page 173.

Step 8 Click **Copy**.

A message appears at the bottom right corner on the CDO screen on a successful copy.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Copy a Rule Across ASA Access Lists and Devices

You can copy an access control rule from one access list to another, either within the same ASA device or across different ASA devices managed in your CDO tenant.

Note The paste operation fails if you attempt to add a rule that already exists in the access list.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, select an access list that you want.

Step 5 Select a rule by clicking the corresponding check box and in the **Actions** pane on the right, click **Copy**.

Step 6 Perform the following:

- To paste the rule within the same ASA device, from the **Selected Access List** drop-down list, select an access list you want.
- To paste the rule to a different ASA device, in the left pane, go to **Inventory** > select an ASA device > **Policy** > **Selected Access List**.

Step 7 To paste the copied rule in the desired position, select a rule that comes after where you want the new rule to be. In the **Actions** pane on the right, click **Paste**. The copied rule will be inserted before the selected rule.

You can use the **Move Up** and **Move Down** buttons to position the rule as needed.

Note Alternatively, you can hover over a desired position in the rule listing table until you see **Paste Rule Here**, and then click it.

Unshare a Shared ASA Access Control List

If the rules governing the interface handling your network become outdated, you can unshare the access control list from the devices currently linked. Unsharing an ASA device from the shared access control list will not have any impact on other ASA devices currently sharing this list.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane on the right, click **Share**.

Step 6 Uncheck the ASA devices that share the selected access list and click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

View ASA Access Policies Listing Page

Note This view applies to ASA devices that have been migrated to the new policy view. For devices that remain onboarded in the legacy policy view, you will continue to see the old view.

The ASA access policy listing page shows a comprehensive overview of all access lists associated with the ASA devices that have been onboarded to the CDO tenant.

Note Click the filter ( ) button, then click **Filter by Device** to search for policies that are either shared across multiple ASA devices or specific to a single ASA device.

Step 1 In the left pane, choose **Policies** > **ASA Access Policies**.

The page provides the following information:

- **Name**: The name of the access list.
- **Device**: The corresponding ASA devices associated with each access list. Additionally, for access lists that are shared across multiple devices, it displays a list of all ASA devices that use the shared access list.

  Click the button to view the ASA devices associated with the selected access list.

  To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

  To return to this page, click **ASA Access Policies**.
- **Interfaces**: The network interfaces to which each access list is assigned.

Step 2 To view the ASA devices associated with an access list, click the corresponding button in the **Device** column.

Step 3 To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

Step 4 To return to the policy listing page, in the top-left corner, click ← **ASA Access Policies**.

Global Search of ASA Access Lists

Use the Global Search functionality to search the following in your CDO tenant:

- ASA devices and all their associated access lists.
- Access lists or shared access lists and their occurrences across all onboarded ASA devices.

Rename an ASA Access Control List

It is possible to modify the name of an access list to suit your specific needs. Whether you want to rename a global access list or a shared access control list, it is a straightforward process. If the access list is shared, changing its name updates the name on all the other devices where the shared access control list is used. Remember that the updated name will only reflect after the configuration is deployed to those devices.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list that you want to rename.

Step 5 Click the **Rename** ( ) icon in the right pane.

Step 6 Click the **Save** ( ) button.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Delete a Rule from an ASA Access Control List

You can remove access rules from the access list, but at least one rule must remain for the list to exist.

Step 1 On the navigation pane, click **Inventory**.

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 Click an access list and select the rules to be deleted.

Step 5 In the **Actions pane** on the right, click **Remove**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Delete an ASA Access Control List

This procedure can be used to delete the access control list, shared access list, or a global access list. Deleting a shared access list from one device does not impact other devices where the access list is in use. On those devices, the access list persists as a local access list.

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane displayed on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list you want to delete.

Step 5 In the **Actions** pane on the right, click **Delete**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Hit Rates

CDO enables you to evaluate the outcome of policy rules, on top of secure and scalable orchestration of policies, providing a simple visualization for more accurate policy analysis and an immediate, actionable pivot to root cause, all in a single pane from the cloud. The Hit Rates feature enables you to:

- Eliminate obsolete and never-matched policy rules, increasing security posture.
- Optimize firewall performance by instantly identifying bottlenecks as well as ensuring correct and efficient prioritization is enforced (for example, most triggered policy rule is prioritized higher).
- Maintain a history of Hit Rates information, even upon device or policy rule reset, for a configured data retention period (1 year).
- Strengthen validation of suspected shadow and unused rules based on actionable information. Removing doubt about update or delete.

- Visualize policy rule usage in the context of the entire policy, leveraging predefined time intervals (day, week, month, year) and scale of actual hits (zero, >100, >100k, etc.) to evaluate impact on packets traversing the network.

View Hit Rates of ASA Policies

Step 1 Select **Policies** > **ASA Access Policies** from the CDO menu bar.

Step 2 Click the filter icon and pin it open.

Step 3 In the Hits area, click the various hit count filters to display which policies are being hit more or less often than others.

Search and Filter ASA Network Rules in the Access List

Search

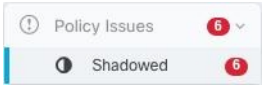
Use the search bar to search for names, keywords, or phrases in the names of the rules within the access list. Search is not case-sensitive.

Filter

Use the filter sidebar to find network policy issues. Filtering is not additive, each filter setting acts independently of the other.

Policy Issues

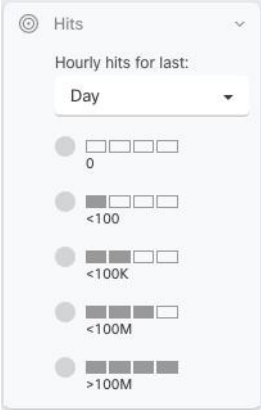
CDO identifies network policies that contain shadow rules. The number of policies that contain shadow rules is indicated in the **Policy Issues** filter:



CDO marks shadowed rules and network policies that contain them with the shadow badge shadow_badge.png on the network policies page. Click Shadowed to view all the policies containing shadow rules. See Shadow Rules for more information.

Hits

Use this filter to find rules across the access lists that have been triggered a number of times over a specified period.



Filter Use Cases

Find all rules that have zero hits

If you have rules without any hits, you can edit them to make them more effective or simply delete them.

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select 0 hits.

Find out how often rules in a network policy are being hit

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hits filters to see what category the different rules fall into.

Filter network policies by hit rate

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hit rate categories. CDO displays the rules that are getting hit at the rate you specify.

Shadowed Rules

A network policy with shadowed rules is one in which at least one rule in the policy will never trigger because a rule that precedes it prevents the packet from being evaluated by the shadowed rule.

For example, consider these network objects and network rules in the "example" network policy:

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100
```

```
access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

No traffic is evaluated by this rule,

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

because the previous rule,

```
access-list example extended deny ip any4 object 02-50
```

denies any ipv4 address from reaching any address in the range 10.10.10.2 - 10.10.10.50.

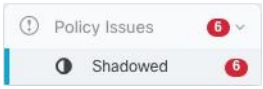
Find Network Policies with Shadowed Rules

To find network policies with shadowed rules, use the network policies filter:

Step 1 In the navigation pane, click **Policies** > **ASA Policies**.

Step 2 Click the filter icon at the top of the ASA Access Policies table.

Step 3 In the Policy Issues filter, check **Shadowed** to view all the policies with shadowed rules.



Resolve Issues with Shadowed Rules

This is how CDO displays the rules described in the "example" network policy above:

The rule on line 1 is marked with a shadow warning badge ⚠ because it's shadowing another rule in the policy. The rule on line 2 is marked as being shadowed ◑ by another rule in the policy. The action for the rule on line 2 is grayed-out because it's entirely shadowed by another rule in the policy. CDO is able to tell you which rule in the policy shadows the rule in line 2.

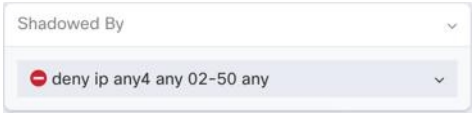
The rule on line 3 can only be triggered some of the time. This is a partially shadowed rule. Network traffic from any IPv4 address trying to reach an IP address in the range 10.10.10.2-10.10.10.50 would never be evaluated because it would have already been denied by the first rule. However, any IPv4 address attempting to reach an address in the range 10.10.10.51-10.10.10.100 would be evaluated by the last rule and would be permitted.

⚠

Caution CDO does not apply a shadow warning badge ⚠ to partially shadowed rules.

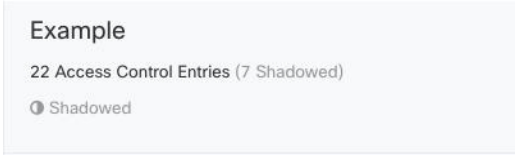
Step 1 Select the shadowed rule in the policy. In the example above, that means clicking on line 2.

Step 2 In the rule details pane, look for the **Shadowed By** area. In this example, the **Shadowed By** area for the rule in line 2 shows that it is being shadowed by the rule in line 1:



Step 3 Review the shadow*ing* rule. Is it too broad? Review the shadow*ed* rule. Do you really need it? Edit the shadow*ing* rule or delete the shadow*ed* rule.

Note By deleting shadowed rules, you reduce the number of access control entries (ACEs) on your ASA. This frees up space for the creation of other rules with other ACEs. CDO calculates the number of ACEs derived from all the rules in a network policy and displays that total at the top of the network policy details pane. If any of the rules in the network policy are shadowed, it also lists that number.



CDO also displays the number of ACEs derived from a single rule in a network policy and displays that information in the network policy details pane. Here is an example of that listing:

Step 4 Determine which devices use the policy by looking in the Devices area of the network policy details pane.

Step 5 Open the **Inventory** page and **Deploy Changes** back to the devices affected by the policy change.

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 Cisco Defense Orchestrator 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 16: 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.

Table Section	Rule Type	Order of Rules within the Section
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."
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 185.

Create a NAT Rule by using the NAT Wizard

Before you begin

See Network Address Translation Wizard, on page 185 for the prerequisites needed to create NAT rules using the NAT wizard.

Step 1 In the left pane, 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 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 102. 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 186
- Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address, on page 188
- Make a Server on the Inside Network Available on a Specific Port of a Public IP Address, on page 189
- Translate a Range of Private IP Addresses to a Range of Public IP Addresses, on page 192

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 194

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.

Step 1 In the left pane, 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 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.

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 servername_outside
host 209.165.1.29
```

```
object network servername_inside
host 10.1.2.29
```

NAT rules created by this procedure:

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

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.

Step 1 In the left pane, 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 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 ASA Network Objects and Network Groups for instructions.

NAT Incoming FTP Traffic to an FTP Server

Step 1 In the left pane, 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 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.

Entries in the ASA's Saved Configuration File

Here is the entry that is created and appears in the ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network ftp-object
host 10.1.2.27
```

NAT rule created by this procedure

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

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 ASA Network Objects and Network Groups for instructions.

Step 1 In the left pane, 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 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.

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.

Object created by this procedure

```
object network http-object
host 10.1.2.28
```

NAT rule created by this procedure

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

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 ASA Network Objects and Network Groups for instructions.

Step 1 In the left pane, 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 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.

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.

Object created by this procedure

```
object network smtp-object
host 10.1.2.29
```

NAT rule created by this procedure

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

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.

For the ASA, the "original address" pool, (the pool of private IP addresses you want to translate) can be a network object with a range of addresses, a network object that defines a subnet, or a network group that includes all the addresses in the pool. For the FTD, the "original address" pool can be a network object that defines a subnet or a network group that includes all the addresses in the pool.

Note For the ASA , 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 ASA Network Objects and 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.**

Step 1 In the left pane, 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 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.

Entries in the ASA's Saved Configuration File

These are the entries that would appear in an ASA's saved configuration file as a result of these procedures.

Note This does not apply to FDM-managed devices.

Objects created by this procedure

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

NAT rules created by this procedure

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

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.

When creating the network objects or network groups, use Create or Edit ASA Network Objects and 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.

Step 1 In the left pane, 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 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.

Entries in the ASA's Saved Configuration File

These are the entries that would appear in an ASA's saved configuration file as a result of these procedures.

Note This does not apply to FDM-managed devices.

Objects created by this procedure

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

NAT rules created by this procedure

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

ASA Templates

Templates enable users to construct a device/service configuration generically, so that they can apply that configuration to others that have been grouped together. These templates provide a single location to make a change in order to impact the many implementers that are grouped together.

ASA Template Parameters

When creating a new template, you may want to model it after a particular device. CDO offers the ability to set template parameters based on selected fields of text within the configuration of the device that the template is modeled after. Parameters can be created, set up from existing parameters, and searched for within the template parameters view.

Note If you opt to import a configuration for an ASA template, the configuration must be in a JSON format.

Create New Parameters

Step 1 With an existing device onboarded, navigate to the **Templates** tab at the top of CDO.
Step 2 Either select **New Template** or **Manage Templates.**
Step 3 Choose the desired configuration to create a parameter.
Step 4 Name the template by typing in the Name field at the top of the screen.
Step 5 Select the desired text field to add a parameter to.
Step 6 Give the parameter a description, add a value, and any necessary note.
Step 7 Click **Save** next to the Name field to save the parameter.
Step 8 You can then review the template by clicking **Review Template.**

You now have a saved parameter that gets applied to all future devices that are onboarded using this template.

Create a New ASA, ISR, or ASR Template

Base Configuration

Start with a known ASA, ISR, or ASR base configuration. Choose the desired configuration to begin parameterization of the template. Parameterization involves selecting fields or attributes within a configuration file and identifying a list of values which will be selected on configuration file instantiation.

Note If you opt to import a configuration for an ASA template, the configuration must be in a JSON format.

Add Parameters

With the selection of a base configuration the parameterization process can begin. From the configuration editor, select the desired field for parameterization. Note that the selected string is enclosed in double brackets. From the left pane, the parameter can be renamed, a description added, and multiple values added. Selecting **Allow Custom Value** allows for custom values to be set on instantiation. Otherwise, only the identified values are selectable.

Once parameterization is completed, identify a name for the template, and click **Save**.

Read more on parameterization ASA Template Parameters.

Review

Once a template has been saved, click **Review** to move to the review process. In review, the template can be exported as-is, including the parameterized values. Note that this is not necessarily a valid configuration but provides a means to review the template as it is stored in CDO. The template can also be edited by clicking **Edit**, if needed. The **Diff** button can demonstrate the differences between the saved template and the most recent edits.

Generate ASA Configurations from Templates

Create a Configuration from a Template

Select the **Config from Template** button to begin the process of generating a custom configuration from a template. Available templates are listed, select the chosen template and click **Choose Template**.

In most cases, templates will contain parameterized values which must be set on **Export** to provide the customized configuration. From the left hand pane, select each parameter and value as desired for this configuration. Notice the values are demonstrated in the editor. These are the values that will replace the parameter on export. With all parameter values set, click on the **Export** button to export the configuration and download. If the template contains no parameterized values, click the **Export** button to export the configuration as is.

Manage ASA Templates

The Manage Templates view gives you the ability to visualize all of your existing templates as well as edit and delete them. Parameterization and value configuration can be modified while editing templates. Simply hover over an existing template and select **Edit** to make changes.

Edit Templates

Once in the edit view:

- Add parameters by double-clicking or highlighting text in the editor.
- Describe the parameter by typing in the description text box. Then click **Add Value**.
- Provide a value and write a note. Click **Add**.
- When you are done, click **Save**.
- You can now review the template by clicking **Review Template**.
    - You can compare the files by clicking **Diff**.
    - To export the template, click **Export**.

API Tokens

Developers use CDO API tokens when making CDO 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 CDO. 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 CDO 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 CDO 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

Migrating an ASA Configuration to an FDM-Managed Device Template

Attention Firepower 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 Defense Orchestrator helps you migrate your ASA to an FDM-managed device. CDO 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 CDO. 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 Defense Orchestrator for a full explanation of the process of migrating an ASA to an FDM-managed device using CDO.

Manage ASA Certificates

Digital certificates provide digital identification for authenticating devices and individual users. 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. For more information on digital certificates, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Certificate Authorities (CAs) are trusted authorities that "sign" certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs also issue identity certificates.

- **Identity Certificate** — 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. CAs issue identity certificates, which are certificates for specific systems or hosts.
- **Trusted CA Certificate** — Trusted 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. A trusted CA certificate is self-signed and called a root certificate.

The Remote Access VPN uses digital certificates for authenticating secure gateways and AnyConnect clients (endpoints) to establish a secure VPN connection. For more information, see Remote Access VPN Certificate-Based Authentication.

Guidelines for Certificate Installation

Read the following guidelines for certificate installation on ASA:

- Certificate can be installed on a single or multiple ASA devices simultaneously.
- Only one certificate can be installed at a time.
- Certificate can be installed only on a live ASA device and not on a modal device.

Install ASA Certificates

You must upload the digital certificates as Trustpoint Objects and install them on the ASA devices managed by CDO.

Note Ensure that the ASA device has no out-of-band changes, and all staged changes have been deployed.

The following lists the digital certificates and formats supported by CDO:

- Identity Certificate can be installed using the following methods:

    - PKCS12 file import.
    - Self-Signed certificate
    - Certificate Signing Request (CSR) import.
- Trusted CA Certificate can be installed using PEM or DER format.

Watch the screencast demonstrates the steps for installing certificates on ASA using CDO. It also shows steps for modifying, exporting, and deleting installed certificates.

Supported Certificate Formats

- PKCS12: PKCS#12, P12, or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as **.pfx** and **.p12**.
- PEM: PEM (originally “Privacy Enhanced Mail”) files contain ASCII (or Base64) encoding data and the certificate files can be in .pem, .crt, .cer, or .key formats. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements.
- DER: DER (Distinguished Encoding Rules) format is simply a binary form of a certificate instead of the ASCII PEM format. It sometimes has a file extension of **.der**, but it often has a file extension of **.cer**, so the only way to tell the difference between a DER .cer file and a PEM .cer file is to open it in a text editor and look for the BEGIN/END statements. Unlike PEM, DER-encoded files do not contain plain text statements such as -----BEGIN CERTIFICATE-----.

Trustpoints Screen

After onboarding the ASA device into CDO, on the **Inventory** tab, select the ASA device and in the **Management** pane on the left, click **Trustpoints**.

In the **Trustpoints** tab, you'll see the certificates that are already installed on the device.

- The "Installed" status indicates that the corresponding certificate is installed successfully on the device.
- The "Unknown" status indicates that the corresponding certificate doesn't contain any information. You need to remove and upload it again with the correct details. CDO discovers all the unknown certificates as trusted CA certificates.
- Click the row that shows "Installed" to view certificate details on the right pane. Click **more** to see additional details of the selected certificate.
- An installed Identity Certificate can be exported in PKCS12 or PEM format and imported into other ASA devices. See Exporting an Identity Certificate.
- Only the advanced settings can be modified on an installed certificate.
    - Click **Edit** to modify the advanced settings.
    - After making the changes, click **Send** to install the updated certificate.

Install an Identity Certificate Using PKCS12

You can select an existing trustpoint object created for PKCS12 format and install it on the ASA device. You can also create a new trustpoint object from the installation wizard and install the certificate on the ASA device.

Before you begin

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

Step 1 In the navigation bar, click **Inventory**.

Step 2 To install an identity certificate on a single ASA device, do the following:

a) Click the **Devices** tab.
b) Click the **ASA** tab and select an ASA device.
c) In the **Management** pane on the right, click **Trustpoints**.
d) Click **Install**.

Note You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

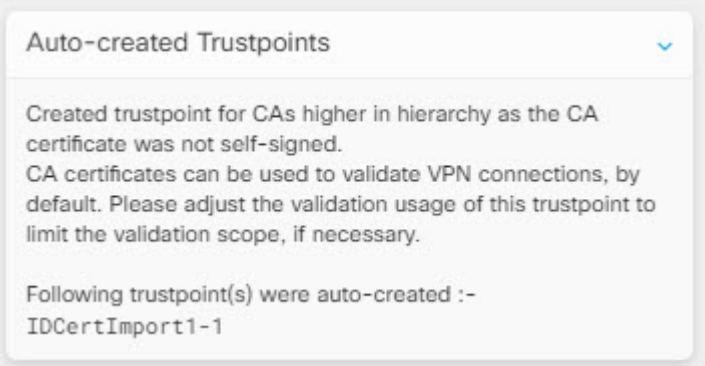
Step 3 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object. For more information, see Adding an Identity Certificate Object Using PKCS12.
- **Choose** to select Certificate Enrollment Object of the PKCS type.

Step 4 Click **Send**.

This installs the certificate on the ASA device

Note If you are importing a PKCS12 certificate that has intermediate CAs installed on it, ASA automatically creates and installs trustpoint objects on the device for every intermediate CA certificate that is not installed already. When you click on the identity certificate, you'll see a message on the right pane, as shown in the following example.



Install a Certificate Using Self-Signed Enrollment

You can select an existing trustpoint object created for a self-signed certificate and install it on the ASA device. You can also create a new trustpoint object from the installation wizard and install the certificate on the ASA device.

Before you begin

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

Step 1 In the navigation bar, click **Inventory**.

Step 2 To install an identity certificate on a single ASA device, do the following:

a) Click the **Devices** tab.
b) Click the **ASA** tab and select an ASA device.
c) In the **Management** pane on the right, click **Trustpoints**.
d) Click **Install**.

Note You can also install a signed certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Step 3 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object. For more information, see Adding an Identity Certificate Object Using PKCS12.
- **Choose** to select a Certificate Enrollment Object of the type Self-Signed..

Step 4 Click **Send**.

For self signed enrollment type trustpoints, the Issuer Common Name status will always be the ASA device since the managed device is acting as its own CA and does not need a CA certificate to generate its own Identity Certificate.

Manage a Certificate Signing Request (CSR)

You must first generate a CSR request and then get this request signed by a trusted Certificate Authority (CA). Then, you can install the signed identity certificate issued by the CA on the ASA device.

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

The following diagram depicts the workflow for generating CSR and installing a certified issued certificate in ASA:

Generate a CSR Request

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 To install an identity certificate on a single ASA device, do the following:

Step 5 Click **Install**.

Step 6 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint CSR object. For more information, see Adding an Identity Certificate Object for Certificate Signing Request (CSR), on page 115.
- **Choose**to select the CSR request trustpoint that is already created..

Step 7 Click **Send**.

This generates an unsigned Certificate Signing Request (CSR).

Step 8 Click the copy icon copy_icon.png to copy the CSR details. You can also download the CSR request in ".csr" file format.

Step 9 Click **OK**.

Step 10 Submit the certificate signing request (CSR) to the Certificate Authority to sign the certificate.

Install a Signed Identity Certificate Issued by a Certificate Authority

Once the CA issues the signed certificate, install it on the ASA device

Step 1 In the **Trustpoint** screen, click the CSR request with the **Status** as "Awaiting Signed Certificate Install" and in the **Actions** pane on the right, click **Install Certified ID Certificate**.

Step 2 Upload the signed certificate received from the CA. You can drag and drop the file or paste its contents in the provided field. The trustpoint commands are generated based on the trustpoint you selected.

Step 3 Click **Send**.

This installs the signed identity certificate to the ASA device. Installing certificates will immediately deploy changes to the device.

Note You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Install a Trusted CA Certificate in ASA

Before you begin

- Read the Guidelines for Certificate Installation.

- ASA must be “Synced” state and “Online”.

Step 1 In the navigation menu, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 To install an identity certificate on a single ASA device, do the following:

a) Select an ASA device and in the **Management** pane on the right, click **Trustpoints**.

b) Click **Install**.

Note You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Step 5 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object. For more information, see Adding a Trusted CA Certificate Object, on page 117.
- **Choose**select a Trusted Certificate Authority Object.

Step 6 Click **Send**.

This installs the trusted CA file on the ASA device.

Export an Identity Certificate

You can export and import the keypair and issued certificates associated with a trustpoint in PKCS12 or PEM format. This format is useful to manually duplicate a trustpoint configuration on a different ASA.

Step 1 In the navigation menu, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA**.

Step 4 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 5 Click the identity certificate to export the certificate configuration. Alternatively, you can search for the certificate by entering its name in the search field.

Step 6 In the **Actions** pane on the right, click **Export Certificate**.

Step 7 Choose the certificate format by clicking the **PKCS12 Format** or the **PEM Format**.

Step 8 Enter the encryption passphrase used to encrypt the PKCS12 file for export.

Step 9 Confirm the encryption passphrase.

Step 10 Click **Export** to export the certificate configuration.

An information dialog box appears, informing you that the certificate configuration file has been successfully exported to the location that you specified.

What to do next

If you want to view the downloaded identity certificate, execute the following commands in the directory where the certificate was downloaded:

1. To decode certificate in base64 format:

   ```
   openssl base64 -d -in <file_name>.p12 -out <file_name>_b64.p12
   ```

2. To view certificate:

   ```
   openssl pkcs12 -in <file_name>_b64.p12 -passin pass:<password>
   ```

Edit an Installed Certificate

You can modify only the advanced options of the installed certificate.

Step 1 In the navigation menu, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the **ASA** tab.
Step 4 Select the ASA device and in the **Management** on the right, click **Trustpoints**.
Step 5 Click the certificate to modify and in the **Actions** pane on the right, click **Edit**.
Step 6 Modify the required parameters and click **Save**.

Delete an Existing Certificate from ASA

You can delete a certificate one after another. After deleting a certificate, it cannot be restored.

Step 1 In the navigation menu, click **Inventory**.
Step 2 Select the ASA device and in the **Management** on the right, click **Trustpoints**.
Step 3 Click the certificate to be deleted and in the **Actions** pane on the right, click **Remove**.
Step 4 Click **OK** to remove the selected certificate.

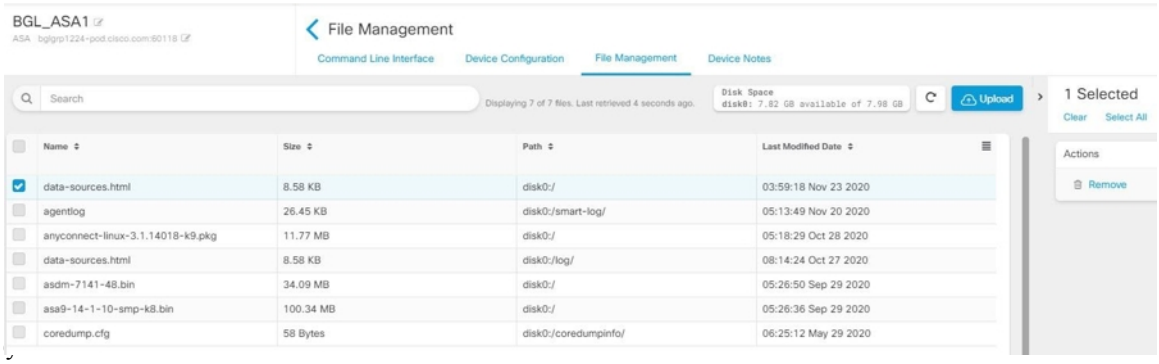
ASA File Management

CDO provides the file management tool to help you perform basic file management tasks such as viewing, uploading, or deleting files present on the ASA device's flash (disk0) space.

Note You cannot manage files present on disk1.

The File Management screen lists all the files present on the device's flash (disk0). On a successful file upload, you can click the refresh icon to see the file. By default, this screen refreshes automatically every 10 minutes.

The **Disk Space** field shows the amount of disk space on the disk0



You can upload the AnyConnect image to single or multiple ASA devices. After a successful upload, the AnyConnect image is associated with the RA VPN configuration on the selected ASA devices. This helps you to upload the newly released AnyConnect package to multiple ASA devices simultaneously.

Upload File to the Flash System

CDO supports only URL based file upload from the remote server. The supported protocols for uploading the file are HTTP, HTTPS, TFTP, FTP, SMB, or SCP. You can upload any files such as the AnyConnect software images, DAP.xml, data.xml, and host scan image files to a single or multiple ASA device.

Note CDO doesn't upload the file to selected ASA devices if the remote server's URL path is invalid or for any issues that may occur. You can navigate to the device **Workflows** for more details.

Suppose the device is configured for High Availability, CDO uploads the file to the standby device first, and only after a successful upload, the file is uploaded to the active device. The same behavior applies during the file removal process.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://rootcisco123@10.10.16.6//root/events_send.py

Before You Begin

- Make sure that the remote server is accessible from the ASA device.
- Make sure that the file is already uploaded to the remote server.

- Make sure that there is a network route from the ASA device to that server.
- If FQDN is used in the URL, make sure that DNS is configured.
- The remote server's URL must be a direct link without prompting for authentication.
- If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Note If you upload a file to an ASA that is configured as a peer in a failover, CDO does not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for CDO to recognize the file in both devices.

Upload File to a Single ASA Device

Use this procedure to upload a file to a single ASA device.

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 In the **Management** pane on the right, click **File Management**. You can view available disk space and the files present on the ASA device.

Step 5 Click the **Upload** button on the right.

Step 6 In the **URL link**, specify the server's path where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:/**DAPFiles/dap.xml" in the field.

Note You can view the directories present in the disk0 folder by executing the **dir** command in the CDO ASA CLI interface.

Step 7 If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled. **Note**: This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, CDO associates the AnyConnect file to the RA VPN configuration on the selected ASA device after a successful upload.

Step 8 Click **Upload**. CDO uploads the file to the device.

Step 9 If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 5, Deploy Configuration Changes from CDO to ASA.

What to do next

You don't have to deploy the configuration changes on the device.`

Upload File to Multiple ASA Devices

Use this procedure to upload a file to multiple ASA devices at the same time.

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

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select multiple ASA devices to perform a bulk upload.

Step 4 In the **Device Actions** pane on the right, click **Upload File**. Note: The **Upload File** link appears if ASA devices are online.

Step 5 In the **URL link**, specify the server's paths where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:/**DAPFiles/dap.xml" in the field.

Note You can view the directories present in the disk0 folder by executing the **dir** command in the CDO ASA CLI interface.

Step 6 If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled.

Note This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, CDO associates the AnyConnect file to the RA VPN configuration on the selected ASA devices after a successful upload.

Step 7 Click **Upload**.

Step 8 If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 4, Deploy Configuration Changes from CDO to ASA.

What to do next

You can view the progress of uploading the file on individual devices. Select the ASA device, and in the **Management** pane on the right, click **File Management**. If the file upload is in progress, wait for the operation to complete.

You don't have to deploy the configuration changes on the device.`

Remove Files from ASA

You are not allowed to remove AnyConnect files associated with the RA VPN configuration. You have to disassociate the AnyConnect file from the corresponding RA VPN configuration and then remove the file from the File Management tool.

Note If you upload a file to an ASA that is configured as a peer in a failover, CDOdoes not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for CDO to recognize the file in both devices.

The remove operation deletes the selected files permanently from the flash memory. A message appears when deleting files asking for confirmation. Use the following procedure to remove files from a selected ASA device:

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 In the **Management** pane on the right, click **File Management**.

Step 5 Select the files you want to remove, and under **Actions** on the right, click **Remove**. A maximum of 25 files can be selected. If CDO fails to remove some files, you can see the device **Workflows** to determine the removed and retained files.

Step 6 If you have chosen to remove the AnyConnect package, Deploy Configuration Changes from CDO to ASA.

Managing ASAs with Pre-existing High Availability Configuration

Configuration Changes Made to ASAs in Active-Active Failover Mode

When Cisco Defense Orchestrator) changes an ASA's running configuration with the one staged on CDO, or when it changes the configuration on CDO with the one stored on the ASA, it attempts to change only the relevant lines of the configuration file if that aspect of the configuration can be managed by the CDO GUI. If the desired configuration change cannot be made using the CDO GUI, CDO attempts to overwrite the entire configuration file to make the change.

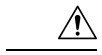
Here are two examples:

- You *can* create or change a network object using the CDO GUI. If CDO needs to deploy that change to an ASA's configuration, it overwrites the relevant lines of the running configuration file on the ASA when the change occurs.
- You *cannot* create a new ASA user using the CDO GUI. If a new user is added to the ASA using the ASA's ASDM or CLI, when that out-of-band change is accepted and CDO updates the stored configuration file, CDO attempts to overwrite that ASA's entire configuration file staged on CDO.

These rules are not followed when the ASA is configured in active-active failover mode. When CDO manages an ASA configured in active-active failover mode, CDO cannot always deploy all configuration changes from itself to the ASA or read all configuration changes from the ASA into itself. Here are two instances in which this is the case:

- **Changes to an ASA's configuration file made in CDO, that CDO does not otherwise support in the CDO GUI, cannot be deployed to the ASA**. Also, a combination of changes made to the configuration file that CDO does not support, along with changes made to the configuration file that CDO does support, cannot be deployed to the ASA. In both cases, you receive the error message, "CDO does not support replacing full configurations for devices in failover mode at this time. Please click Cancel and apply changes to the device manually." Along with the message in the CDO interface, you see a Replace Configuration button that is disabled.

- **Out-of-band changes made to an ASA configured in active-active failover mode will not be rejected by CDO**. If you make an out-of-band change to an ASA's running configuration, the ASA gets marked with "Conflict Detected" on the **Inventory** page. If you review the conflict and try to reject it, CDO blocks that action. You receive the message, "CDO does not support rejecting out-of-band changes for this device. Either this device is running an unsupported software version or is a member of a active/active failover pair. Please proceed to accept the out-of-band changes by clicking Continue."



Caution If you find yourself having to accept out-of-band changes from the ASA, any configuration changes staged on CDO, but not yet deployed to the ASA, will be overwritten and lost.

CDO does support configuration changes made to an ASA in failover mode when those changes are supported by the CDO GUI.

Related Information:

Configure DNS on ASA

Use this procedure to configure a domain name server (DNS) on each of your ASAs.

Prerequisites

- The ASA must be able to reach the internet.
- Before you begin, gather this information:
  - The name of the ASA interface that can reach the DNS server; for example, inside, outside, or dmz.
  - The IP address of the DNS server your organization uses. If you don't maintain your own DNS server, you can use Cisco Umbrella. The IP address for Cisco Umbrella is 208.67.220.220.

Procedure

Step 1 In the navigation bar, click**Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select all the ASAs on which you want to configure DNS.

Step 4 In the Actions pane to the right, select **Command Line Interface**.

Step 5 Click the CLI macro favorites star.

Step 6 Select the **Configure DNS** macro in the Macros panel.

Step 7 Se;ect **>_View Parameters** and in the parameters column, fill in the values for these parameters:

- IF_Name - The name of the ASA interface that can reach the DNS server.
- IP_ADDR - The IP address of the DNS server your organization uses.

Step 8 Click **Send to devices**.

CDO Command Line Interface

CDO provides users with a command line interface (CLI) for managing ASA devices. Users can send commands to a single device or to multiple devices simultaneously.

Related Information:

- For detailed ASA CLI documentation, see ASA Command Line Interface Documentation, on page 224.

Using the Command Line Interface

Step 1 Open the **Inventory** page.

Step 2 Click the **Devices** button abobve the Inventory table.

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 212

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 CDO 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 ASA **device Commands**: CDO executes commands in ASA's Global Configuration mode.

Long Commands: If you enter a very long command, CDO attempts to break up your command into multiple commands, so that they can all be run against the API. If CDO is unable to determine a proper separation of your command, it will prompt you for a hint on where to break the list of commands. For example:

```
Error: CDO attempted to execute a portion of this command with a length that exceeded 600
characters. You can give a hint to CDO at where a proper command separation point is by
breaking up your list of commands with an additional empty line between them.
```

If you receive this error:

Step 1 Click the command in the CLI history pane that caused error. CDO populates the command box with the long list of commands.

Step 2 Edit the long list of commands by entering an empty line after groups of related commands. For example, add an empty line after you define a list of network objects and add them to a group like in the example above. You may want to do this at a few different points in the list of commands.

Step 3 Click **Send**.

Work with Command History

After you send a CLI command, CDO 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:

Step 1 On the **Inventory** page, select the device you want to configure.

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**. CDO displays the results of the command in the response pane.

Note CDO 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, CDO returns `Done!`.

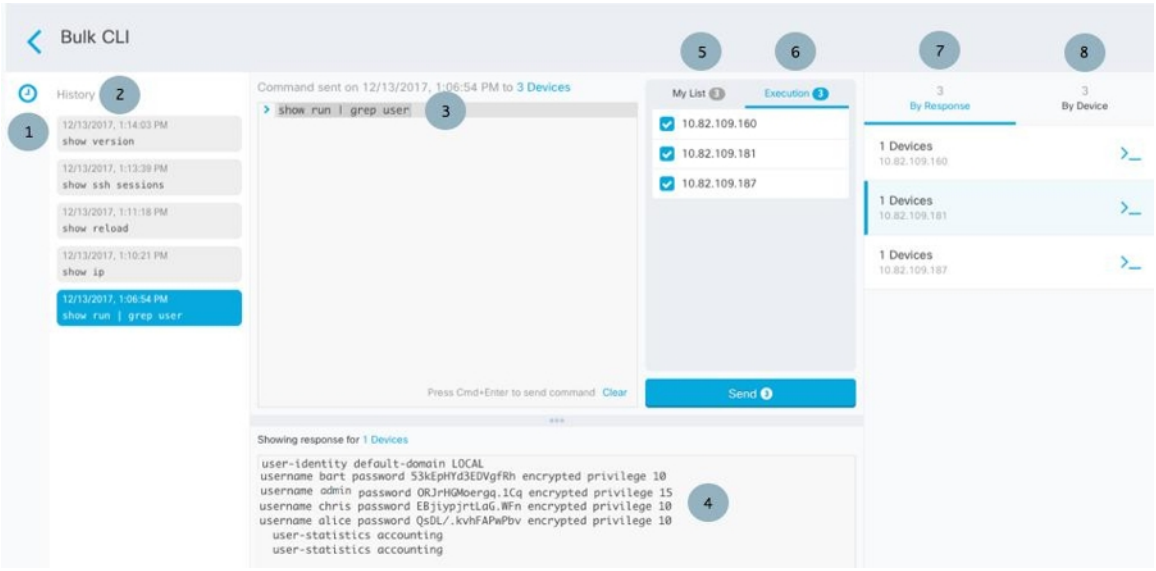
Bulk Command Line Interface

CDO 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 detailed documentation on the ASA CLI documentation, see ASA Command Line Interface Documentation, on page 224.

Bulk CLI Interface



Note CDO 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, CDO returns **Done!**.

Number	Description
1	Click the clock to expand or collapse the command history pane.
2	Command history. After you send a command, CDO records the command in this history pane so you can return to it, select it, and run it again.

Number	Description
3	Command pane. Enter your commands at the prompt in this pane.
4	Response pane. CDO displays the device's response to your command as well as CDO 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 CDO displays all the devices that returned the same response to the command. **Note** CDO 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, CDO 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, CDO 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

Step 1 In the navigation bar, click **Inventory**.

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 CDO records your command in the History pane in the Bulk CLI window.

Note A command will succeed on selected ASA devices that are synced and may fail on devices that are not synced. If any of the selected ASA devices are not synced, only the following commands are allowed: `show, ping, traceroute, vpn-sessiondb, changeto, dir, write, and copy.`

Work with Bulk Command History

After you send a bulk CLI command, CDO 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.

Step 1 In the navigation bar, click **Inventory**.

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**. CDO displays the results of the command in the response pane.

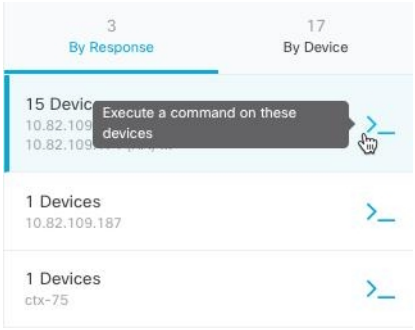
Note A command will succeed on selected ASA devices that are synced and may fail on devices that are not synced. If any of the selected ASA devices are not synced, only the following commands are allowed: `show, ping, traceroute, vpn-sessiondb, changeto, dir, write, and copy.`

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, CDO 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 CDO 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:

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, CDO 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:

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 CDO 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 ASA 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 ASA 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 CDO 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 CDO.

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

Step 1 Before you create a CLI macro, test the command in CDO's Command Line Interface to make sure the command syntax is correct and it returns reliable results.

Note
- For detailed ASA CLI documentation, see ASA Command Line Interface Documentation, on page 224.

Step 2 In the navigation bar, click **Inventory**.

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.

Step 1 In the navigation bar, click **Inventory**.

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

Step 1 In the navigation bar, click **Inventory**.

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 CDO has successfully, sent the command and updated the device's configuration, you receive the message, Done!

- For an ASA the running 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 ASA devices. Macros are not specific to a particular device.

Step 1 In the navigation bar, click **Inventory**.
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.

Step 1 In the navigation bar, click **Inventory**.
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.

Configure ASA Using CDO CLI

You can configure an ASA device by running the CLI commands in the CLI interface provided in CDO. To use the interface, on the **Inventory** menu, select the device and click **Command Line Interface**. For more information, see Using the CDO Command Line Interface.

Add a New Logging Server

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts.

For more information, see the 'Monitoring' section of the 'Logging' chapter in the CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Configure the DNS Server

You need to configure DNS servers so that the ASA can resolve host names to IP addresses. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

For more information, see the 'Basic Settings' chapter of the 'Configure the DNS Server' section in CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Add Static and Default Routes

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing.

For more information, see the 'Static and Default Routes' chapter of CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide.

Configure Interfaces

You can configure the management and data interfaces using CLI commands. For more information, see the 'Basic Interface Configuration' chapter of CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide.

Compare ASA Configurations Using CDO

Use this procedure to compare the configurations of two ASAs.

Step 1 In the navigation menu, click **Inventory**.

Step 2 Click the **Devices** tab to locate the ASA device or the **Templates** tab to locate the ASA model device.

Step 3 Click the **ASA** tab.

Step 4 Filter your device list for the devices you want to compare.

Step 5 Select two of your ASAs. Their status does not matter. You are comparing the configurations of the ASAs stored on CDO.

Step 6 In the Device Actions pane on the right, click **Compare.**

Step 7 In the Comparing Configurations dialog, click **Next** and **Previous** to skip through the differences, highlighted in blue, in the configuration files.

ASA Bulk CLI Use Cases

The following cases are possible workflows you may experience when using CDO's bulk CLI function for ASA devices.

Show all users in the running configuration of an ASA and then delete one of the users

Step 1 In the navigation bar, click **Inventory**.

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

Step 3 Click the **ASA** tab.

Step 4 Search and filter the device list for the devices from which you want to delete the user and **select** them.

Note Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy`, and `write`.

Step 5 Click **>_Command Line Interface** in the details pane. CDO lists the devices you chose in the My List pane. If you decide to send the command to fewer devices, uncheck devices in that list.

Step 6 In the command pane, enter `show run | grep user` and click **Send.** All the lines in the running configuration file that contain the string user will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.

Step 7 Click the By Response tab and review the responses to determine which devices have the user that you want to delete.

Step 8 Click the My List tab and select the list of devices from which you want to delete the user.

Step 9 In the command pane, enter the no form of the user command to delete user2 and then click **Send**. For the sake of this example, you are going to delete user2:

```
no user user2 password reallyhardpassword privilege 10
```

Step 10 Look in the history panel for the instance of the `show run | grep user` command, you used to search for the user name. Select that command, look at the list of devices in the Execution list and select **Send**. You should see that the username has been deleted from the devices you specified.

Step 11 If you are satisfied that you have deleted the correct users from the running configuration and that the correct users remain in the running configuration:

a. Select the `no user user2 password reallyhardpassword privilege 10` command from the history pane.

b. Click the **By Device** tab and click **Execute a command on these devices**.

c. In the command pane, click **Clear** to clear the command pane.

d. Enter the command `deploy memory` and click **Send**.

Find all SNMP configurations on selected ASAs

This procedure shows you all the SNMP configuration entries in the running configuration of the ASA.

Step 1 In the navigation bar, click **Inventory**.

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

Step 3 Click the **ASA** tab.

Step 4 Filter and search for the devices on which you want to analyze the SNMP configuration in the running configuration and **select** them.

Note Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, and `dir`.

Step 5 Click **Command Line Interface** in the details pane. The devices you chose are in the My List pane. If you decide to send the command to fewer devices, uncheck devices in the list.

Step 6 In the command pane, enter `show run | grep snmp` and click **Send.** All the lines in the running configuration file that contain the string snmp will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.

Step 7 Review the command output in the response pane.

ASA Command Line Interface Documentation

CDO fully supports the ASA command line interface. We provide a terminal-like interface within CDO for users to send ASA commands to single devices and multiple devices simultaneously. The ASA command line interface documentation is extensive. Rather than recreating parts of it in the CDO documentation, here are pointers to the ASA CLI documentation on Cisco.com.

ASA Command Line Interface Configuration Guides

Starting with ASA version 9.1, the ASA CLI Configuration Guide is broken into three separate books:

- CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide
- CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide
- CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide

You can reach the ASA CLI Configuration Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Configure > Configuration Guides.

A Few Specific ASA Command Line Interface Configuration Guide Sections

Filtering show and more Command Output. You can learn about filtering show command output by using regular expressions in CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide under Filter show and more Command Output.

ASA Command Reference

The ASA Command Reference Guide is an alphabetical listing of all the ASA commands and their options. The ASA command reference is not version specific. It is published in four books:

- Cisco ASA Series Command Reference, A - H Commands
- Cisco ASA Series Command Reference, I - R Commands
- Cisco ASA Series Command Reference, S Commands
- Cisco ASA Series Command Reference, T - Z Commands and IOS Commands for the ASASM

You can reach the ASA Command Reference Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Reference Guides > Command References > ASA Command References.

Export CDO 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:

Step 1 In the navigation bar, click**Inventory**.

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:

Step 1 Open the **Inventory** page.
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:

Step 1 In the navigation pane, click **Inventory**.
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:

- CDO Command Line Interface, on page 212
- Create a CLI Macro from a New Command
- Delete a CLI Macro
- Edit a CLI Macro
- Run a CLI Macro
- ASA Bulk CLI Use Cases

- ASA 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:

Step 1 In the navigation pane, click **Inventory**.

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.

Restore an ASA Configuration

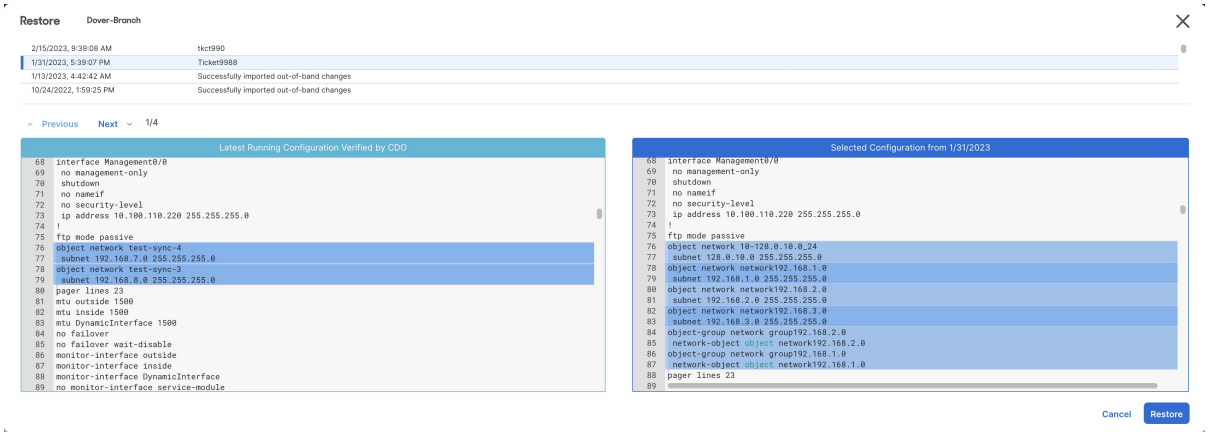
If you make a change to an ASA's configuration, and you want to revert that change, you can restore an ASA's past configuration. This is a convenient way to remove a configuration change that had unexpected or undesired results.

About Restoring an ASA Configuration

Review these notes before restoring a configuration:

- CDO compares the configuration you choose to restore with the last known configuration deployed to the ASA, it does not compare the configuration you choose to restore with a configuration that is staged but not deployed to the ASA. If you have any undeployed changes on your ASA and you restore a past configuration, the restore process will overwrite your undeployed changes and you will lose them.
- Before you can restore a past configuration, the ASA can be in a Synced or Not Synced state but if the device is in a Conflict Detected state, the conflict must be resolved before you restore a past configuration.
- Restoring a past configuration overwrites all intermediate deployed configurations changes. For example, restoring the configuration from 1/31/2023 in the list below overwrites the configuration changes made on 2/15/2023.
- Clicking the Next and Previous buttons will move you through the configuration file and highlight the configuration file changes
- If you originally applied a change request label to your configuration changes, that label appears in the Restore Configuration list.

Figure 4: ASA Restore Configuration Screen



How Long are Configuration Changes Kept?

You can restore an ASA configuration that is 1 year old or less. CDO restores configuration changes logged in its changelog. The change log records changes every time a configuration change is written to or read from an ASA. CDO stores 1 year's worth of changelogs and there is no limitation on the number of the backups made within the previous year.

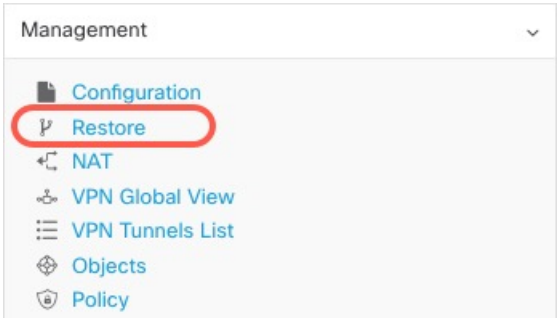
Restore an ASA Configuration

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

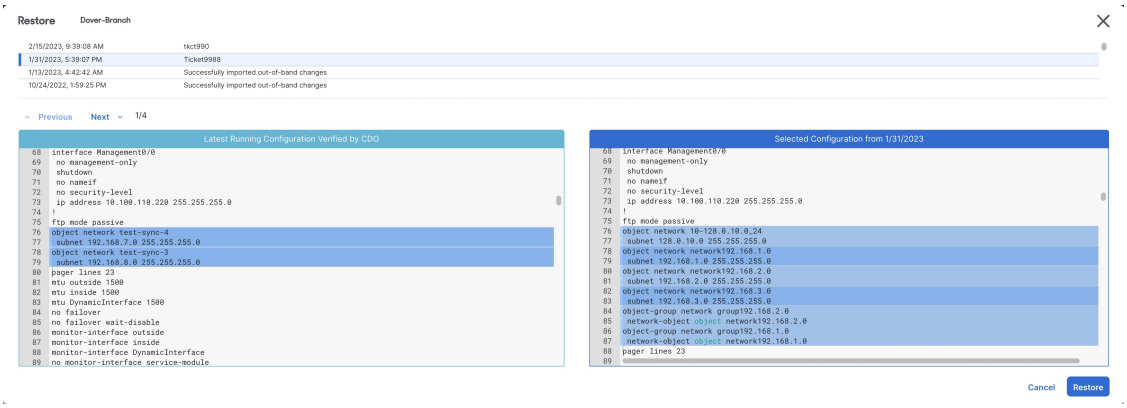
Step 2 Click the ASA tab.

Step 3 Select the ASA whose configuration it is you want to restore.

Step 4 In the **Management** pane, click **Restore.**



Step 5 In the **Restore** page, select the configuration you want to revert to.



For example, in the picture above, the configuration from 1/31/2023 is selected.

Step 6 Compare the "Latest Running Configuration Verified by CDO" and the "Selected Configuration from <*date*>" to ensure you want to restore the configuration displayed in the Selected Configuration from <*date*> window. Use the Previous and Next to compare all the changes.

Step 7 Click **Restore,** this stages the configuration in CDO. On the **Inventory** page, you see that the configuration status of the device is now "Not Synced."

Step 8 Click **Deploy Changes...** in the right-hand pane to deploy the changes and sync the ASA.

Troubleshooting

How do I recover changes I lost but wanted to keep?

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 ASA tab.

Step 4 Select the required device.

Step 5 Click **Change Log** in the right pane.

Step 6 Review the changes in the change log. You may be able to reconstruct your lost configurations from those records.

Manage ASA and Cisco IOS Device Configuration Files

Some types of devices such as the ASA and Cisco IOS devices store their configurations in a single file. For these devices, you can view the configuration file on CDO and perform a variety of operations on it.

View a Device's Configuration File

For the devices which store their entire configurations in a single configuration file, such as ASA, SSH-managed devices, and devices running Cisco IOS, you can view the configuration file using CDO.

Note SSH-managed devices and Cisco IOS Devices have read-only configurations.

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 appropriate device type tab.

Step 4 Select the device or model whose configuration it is you want to view.

Step 5 In the **Management** pane on the right, click **Configuration**.
The full configuration file is displayed.

Related Information:

- Edit a Complete Device Configuration File

Edit a Complete Device Configuration File

Some types of devices store their configurations in a single configuration file, such as ASA . For these devices, you can view the device configuration file on CDO and perform a variety of operations on it depending on the device.

Currently, only ASA configuration files can be edited directly using CDO.

Caution This procedure is for advanced users who are familiar with the syntax of the device's configuration file. This method makes changes directly to copy of the configuration file stored on CDO.

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 **ASA** tab.

Step 4 Select the device whose configuration it is you want to edit.

Step 5 In the **Management** pane on the right, click **Configuration**.

Step 6 In the **Device Configuration** page, click **Edit**.

Step 7 Click the editor button on the right and select the **Default** text editor, **Vim**, or **Emacs** text editors.

Step 8 Edit the file and save the changes.

Step 9 Return to the **Inventory** page and preview and deploy the change.

About Device Configuration Changes

In order to manage a device, CDO must have its own copy of the device's configuration stored in its local database. When CDO "reads" a configuration from a device it manages, it takes a copy of the device's configuration and saves it. The first time CDO 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 CDO. This option allows you to undo all pending changes. The pending changes are deleted and CDO 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 CDO to compare its copy of the device's configuration with the copy of the configuration stored on the device. If there is a difference, CDO 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, CDO checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, CDO 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 CDO's copy of a device's configuration with the latest copy of the configuration stored on the device. CDO 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 CDO with the configurations stored on the devices.

- **Deploy Changes**: As you make changes to a device's configuration, CDO saves the changes you make to its own copy of the configuration. Those changes are "pending" on CDO 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 CDO deploys the changes to the device do they have an effect. When CDO 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, CDO shows you a preview of the pending changes in CDO. Clicking **Discard All** deletes all pending changes from CDO 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 239 for more information.

Read All Device Configurations

If a configuration change is made to a device outside of Cisco Defense Orchestrator (CDO), the device's configuration stored on CDO and the device's local copy of its configuration are no longer the same. You many want to overwrite CDO'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 CDO manages the two copies of the device's configuration.

Here are three configuration statuses where clicking **Read All** will overwrite CDO's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**-If conflict detection is enabled, CDO polls the devices it manages every 10 minutes for changes made to their configurations. If CDO finds that the configuration on the device has changed, CDO displays a "Conflict detected" configuration status for the device.
- **Synced**-If the device is in a synced state, and you click **Read All**, CDO immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, CDO confirms your intent to overwrite its copy of the device's configuration and then CDO performs the overwrite.
- **Not Synced**-If the device is in the Not Synced state, and you click **Read All**, CDO warns you that there are pending changes made to to the device's configuration using CDO and that proceeding with the Read All operation will delete those changes and then overwrite CDO's copy of the configuration with the configuration on the device. This Read All functions like Discard Configuration Changes.

Step 1 In the navigation bar, click **Inventory**.

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 CDO. Notice that CDO only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Click **Read All**.

Step 7 CDO warns you if there are configuration changes staged on CDO, 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 CDO 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 CDO.

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 an ASA to CDO

Why Does Cisco Defense Orchestrator "Read" ASA Configurations?

In order to manage an ASA, CDO must have it's own stored copy of the ASA's running configuration file. The first time CDO reads and saves a copy of the device's configuration file is when the device is onboarded. Subsequently, when CDO reads a configuration from an ASA, you are opting to either **Check for Changes**, **Accept without Review**, or **Read Configuration**. See About Device Configuration Changes for more information.

CDO also needs to read an ASA configuration in these circumstances:

- Deploying configuration changes to the ASA has failed and the device state is not listed or **Not Synced**.
- Onboarding a device has failed and the device state is **No Config**.
- You have made changes to the device configuration outside of CDO and the changes have not been polled or detected. THe device state would be either S**ynced** or C**onflict Detected**.

In these cases, CDO needs a copy of the last known configuration stored on the device.

Read Configuration Changes on ASA

When prompted to Read Configuration changes on an ASA:

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device that CDO has recently failed to onboard or the device that CDO has failed to deploy a change to.

Step 5 Click **Read Configuration** in the Synced pane at the right. This option overwrites the configuration currently saved to CDO.

Preview and Deploy Configuration Changes for All Devices

CDO 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, CDO creates an entry in this page for all on-prem management centers that are managed by CDO.

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.

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 CDO 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 CDO to ASA, on page 234
- Change Log Entries after Deploying to an ASA, on page 323

Deploy Configuration Changes from CDO to ASA

Why Does CDO Deploy Changes to an ASA?

As you manage and make changes to a device's configuration with Cisco Defense Orchestrator (CDO), CDO saves the changes you make to its own copy of the configuration file. Those changes are considered "staged" on CDO until they are "deployed" to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after CDO "deploys" the changes to the device do they have an effect on the traffic running through the device. When CDO 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.

The ASA has a "running" configuration file, sometimes called the "running config" and a "startup" configuration file that is sometimes called the "startup config." The configuration stored in the running config file is enforced on traffic passing through the ASA. After you make changes to the running config and you are happy with the behavior those changes produce, you can deploy them to the startup config. If the ASA is ever rebooted, it uses the startup config as its configuration starting point. Any changes you make to the running config that are not saved to the startup config are lost after an ASA is rebooted.

When you deploy changes from CDO to an ASA, you are writing those changes into the running configuration file. After you are satisfied with the behavior those changes produce, you can deploy those changes to the startup configuration file.

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.

Some Changes are Deployed Directly to the ASA

If you use the CDO Command Line Interface Command Line Interface Macros interface on CDO to make a change to an ASA, those changes are not "staged" on CDO. They are deployed directly to the running configuration of the ASA. When you make changes that way, your device remains "synced" with CDO.

About Deploying Configuration Changes

This section assumes you are using CDO's GUI or editing the Device Configuration page, *not* using CDO's CLI interface or CLI macro interface, to make changes to an ASA configuration file.

Updating an ASA configuration is a two-step process.

Step 1 Make changes on CDO using one of these methods:

- The CDO GUI
- The device configuration on the Device Configuration page

Step 2 After you make your changes, return to the **Inventory** page and then **Preview and Deploy...** the change to the device.

What to do next

When CDO updates an ASA's running configuration with the one staged on CDO, or when it changes the configuration on CDO with the running configuration stored on the ASA, it attempts to change only the relevant lines of the configuration file if that aspect of the configuration can be managed by the CDO GUI. If the desired configuration change **cannot** be made using the CDO GUI, CDO attempts to overwrite the entire configuration file to make the change.

Here are two examples:

- You **can** create or change a network object using the CDO GUI. If CDO needs to deploy that change to an ASA's configuration, it would overwrite the relevant lines of the running configuration file on the ASA when the change occurs.
- You **cannot** create a new local ASA user using the CDO GUI but you can create one by editing the ASA's configuration on the Device Configuration page. If you add a user on the Device Configuration page, and you deploy that change to the ASA, CDO will try to save that change to the ASA's running configuration file by overwriting the entire running configuration file.

Deploy Configuration Changes Made Using the CDO GUI

Step 1 After you make a configuration change using the CDO GUI and save your change, that change is saved in CDO's stored version of the ASA's running configuration file.

Step 2 Return to the device on the **Inventory** page.

Step 3 Click the Devices tab. You should see that the device is now "Not synced."

Step 4 Deploy the changes using one of these methods:

- Click the **Deploy** icon  at the top-right of the screen. This gives you a chance to review the changes you made to the device before you deploy them. Check the device you made changes to, expand the device to review the changes, click **Deploy Now** to deploy the changes.

  Note If you see a yellow warning triangle next to your device on the Devices with Pending Changes screen, you cannot deploy a change to it. Hover your mouse over the warning triangle to learn why you can't deploy changes to the device.

- In the Not Synced pane, click **Preview and Deploy....**

  a. Review the commands that will change the ASA configuration file.

  b. If you are satisfied with the commands, choose a Configuration Recovery Preference.

  Note If you choose "Let me know and I will restore the configuration manually." click **View Manual Synchronization Instructions** before continuing.

  c. Click **Apply Changes to Device**.

  d. Click **OK** to acknowledge the success message.

Schedule Automatic Deployments

You can also configure your tenant to schedule deployments to a single device or all devices with pending changes by Schedule an Automatic Deployment.

Deploy Configuration Changes Using CDO's CLI Interface

Step 1 In the left navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device whose configuration you want to change.

Step 5 Click **>_Command Line Interface** in the **Actions** pane.

Step 6 If there are any commands in the command line interface table, click **Clear** to remove them.

Step 7 In the top box of the command line interface table, enter your commands at the command prompt. You can run a single command, several commands in a batch by entering each command on its own line, or entering a section of configuration file as a command. Here are some examples of commands you can enter in the command line interface table:

A single command creating the network object "albany"

```
object network albany
host 209.165.30.2
```

Multiple commands sent together:

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

A section of a running configuration file entered as a command:

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

Note CDO does not require you to move between EXEC mode, Privileged EXEC mode, and Global Configuration mode. It interprets the command you enter in the proper context.

Step 8 After you have entered your commands, click **Send**. After CDO has successfully deployed the changes to the ASA's running config file, you receive the message, Done!

Step 9 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 **Deploy to Disk** saves the changes made by this command, and any other change in the running config, to the ASA's startup config.
- Clicking **Dismiss**, dismisses the message.

Deploy Configuration Changes by Editing the Device Configuration

Caution This procedure is for advanced users who are familiar with the syntax of an ASA configuration file. This method makes changes directly to the running configuration file stored on CDO.

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device whose configuration you want to change.

Step 5 Click **View Configuration** in the Actions pane.

Step 6 Click **Edit**.

Step 7 Make your changes to the running configuration and **Save** them.

Step 8 Return to the **Inventory** page. In the Not Synced pane, click **Preview and Deploy...**

Step 9 In the Device Sync pane review the changes.

Step 10 Click **Replace Configuration** or **Apply Changes to Device** depending on the kind of change it is.

Deploy Configuration Changes for a Shared Object on Multiple Devices

Use this procedure when you are making changes to a policy or object shared by two or more devices. You can change a common policy on however many devices use it.

Step 1 Open and edit the Policies page or the Objects page containing the shared object you want to edit.

Step 2 Review the shared device list and confirm that you want to make the changes on all the devices mentioned.

Step 3 Click **Confirm**.

Step 4 Click **Save**.

Step 5 Click the **Deploy** icon and Preview and Deploy Configuration Changes for All Devices.

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:

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

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 CDO. 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 239

About Scheduled Automatic Deployments

Using CDO, 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 45 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 CDO 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 CDO, 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.

Step 1 In the navigation bar, click **Inventory**.

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:

Step 1 In the navigation bar, click **Inventory**.

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.

Step 1 In the navigation bar, click**Inventory**.

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 232
- Deploy Configuration Changes from CDO to ASA, on page 234
- Preview and Deploy Configuration Changes for All Devices, on page 233

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 CDO. You will see the this option when the device is in the "Synced" state.

To check changes:

Step 1 In the navigation bar, click **Inventory**.

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 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 CDO.
  - Click **Cancel** to cancel the action.

- For ASA device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on CDO. 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 CDO 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 CDO. When you click **Discard Changes**, CDO *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 CDO will be the same as the copy of the configuration on the device and the configuration status in CDO will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

Step 1 In the navigation bar, click **Inventory**.

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-CDO warns you that "Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-CDO deletes the change immediately.
- For AWS devices-CDO 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 CDO. 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-Prem Firewall Management Center on the On-Prem Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on CDO 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-Prem Firewall Management Center, CDO checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of CDO.

If CDO finds that there are changes to the device's configuration that are not stored on CDO, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When CDO 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 CDO'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-Prem Firewall Management Center, there may be changes made, for instance, to objects outside CDO, which are pending to be synchronized with CDO or changes made in CDO which are pending to be deployed to the On-Prem Firewall Management Center.

Synchronizing Configurations Between CDO and Device

About Configuration Conflicts

On the **Inventory** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Prem Firewall Management Center that you manage using CDO, navigate **Tools & Services** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on CDO) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in CDO was changed and it is now different that the configuration stored locally on the device. Deploying your changes from CDO to the device changes the configuration on the device to match CDO's version.
- Changes made to devices outside of CDO 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 CDO to match the configuration on the device.

Conflict Detection

When conflict detection is enabled, Cisco Defense Orchestrator (CDO) polls the device for the default interval to to determine if a change has been made to the device's configuration outside of CDO. If CDO detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of CDO are called "out-of-band" changes.

In the case of an On-Prem Firewall Management Center that is managed by CDO, if there are changes that are staged and the device is in **Not Synced** state, CDO stops polling the device to check for changes. When there are changes made outside CDO which are pending to be synchronized with CDO and changes made in CDO which are pending to be deployed to the on-prem management center, CDO declares the on-prem 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 246 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of CDO.

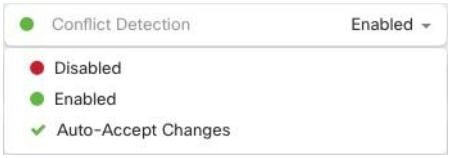
Step 1 In the navigation bar, click **Inventory**.

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 CDO to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using CDO are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on CDO 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, CDO 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, CDO automatically updates its local version of the device's configuration without prompting you.

CDO will ***not*** automatically accept a configuration change if there are configuration changes made on CDO 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 **Inventory** page; then, you enable auto-accept changes for individual devices.

If you want CDO to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection, on page 243 instead.

Configure Auto-Accept Changes

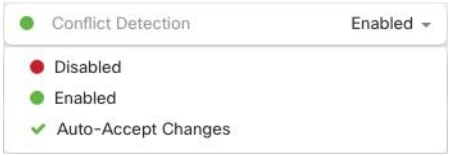
Step 1 Log in to CDO using an account with Admin or Super Admin privileges.

Step 2 In the left pane, click **Settings** > **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 **Inventory** page.

Step 4 Open the **Inventory** page 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

Step 1 Log-in to CDO using an account with Admin or Super Admin privileges.

Step 2 Navigate **Settings** > **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 CDO. 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:

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **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 CDO 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 CDO to the device, or you want to "undo" the configuration changes you started making on CDO. This option overwrites the configuration stored in CDO with the running configuration stored on the device.

Resolve the Conflict Detected Status

CDO allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 243 is enabled and there was a change made to the device's configuration without using CDO, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Conflict Detected** state and continue from Step 4.

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 CDO.
- 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** CDO with the device's running configuration.

  Note As CDO 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 CDO.

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 243 enabled, or if you **Enable the option to auto-accept device changes** from the Settings page,CDO polls the device for the default interval to determine if a change has

been made to the device's configuration outside of CDO. You can customize how often CDO 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 **Inventory** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

After you enable **Conflict Detection** from the **Inventory** page or **Enable the option to auto-accept device changes** from the Settings page, use the following procedure to schedule how often you want CDO to poll your devices:

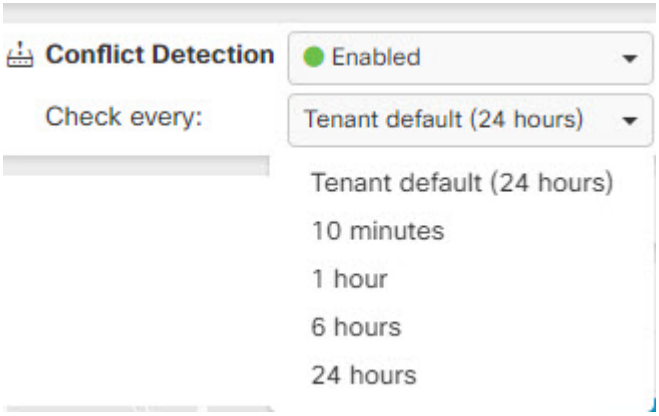
Step 1 In the navigation bar, click **Inventory**.

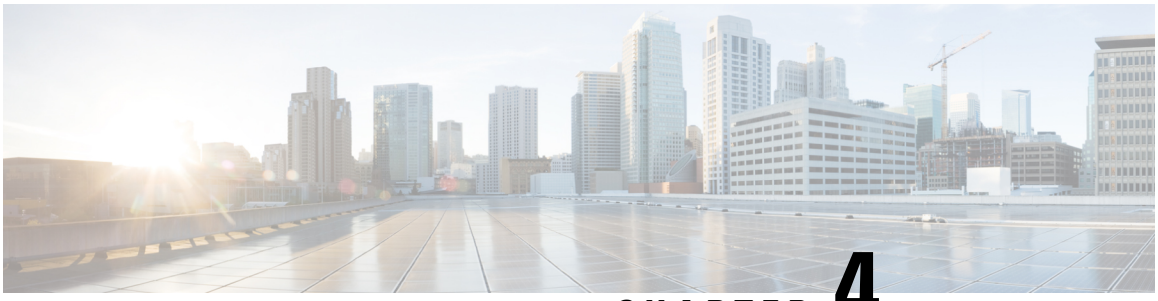
Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

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:





CHAPTER 4

Managing Virtual Private Network in CDO

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 Adaptive Security Appliances (ASA) device. It also describes the SSL standards that are used to build and remote access VPN connections on ASA.

CDO supports the following types of VPN connections:

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 ASA.

IPsec and IKE Protocols

In CDO, 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.

VPN Encryption Domain

There are two methods to define the VPN's encryption domain: route-based or policy-based traffic selectors.

- **Policy-Based**: The encryption domain is set to allow any traffic which enters the IPSec tunnel. IPSec Local and remote traffic selectors are set to 0.0.0.0. This means that any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet. ASA supports policy-based VPN with crypto maps.
- **Route-Based**: The encryption domain is set to encrypt only specific IP ranges for both source and destination. It creates a virtual IPsec interface, and whatever traffic enters that interface is encrypted and decrypted. ASA supports route-based VPN with the use of Virtual Tunnel Interfaces (VTIs).

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 CDO 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:

- Site-to-Site VPN Configuration Between ASAs, on page 250
- Monitor ASA Site-to-Site Virtual Private Networks

Site-to-Site VPN Configuration Between ASAs

Cisco Defense Orchestrator supports these aspects of site-to-site VPN functionality on Adaptive Security Appliance (ASA) 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 the static or dynamic IP address for the extranet device as an endpoint.

Configure Site-to-Site VPN Connections with Dynamically Addressed Peers

CDO 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.
- 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.

Note If the IP address of the interface is changed by using a local manager like Adaptive Security Device Manager (ASDM), the **Configuration Status** of that peer in CDO shows "Conflict Detected". When you Resolve the Conflict Detected Status, the **Configuration Status** of the other peer changes to the "Not Synced" state. You must deploy the CDO 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 scenario:

If a device has more than one dynamic peer connection.

- 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.

ASA Site-to-Site VPN Guidelines and Limitations

- CDO does not support a crypto-acl to design the interesting traffic for S2S VPN. It only supports protected networks.
- 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.

Guidelines for Virtual Tunnel Interfaces

- VTIs are only configurable in IPsec mode. To terminate GRE tunnels on an ASA is unsupported.
- You can use dynamic or static routes for traffic using the tunnel interface.
- The MTU for VTIs is automatically set, according to the underlying physical interface. However, if you change the physical interface MTU after the VTI is enabled, you must disable and reenable the VTI to use the new MTU setting.
- If Network Address Translation has to be applied, the IKE and ESP packets will be encapsulated in the UDP header.
- IKE and IPsec security associations will be re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.
- Tunnel group name must match what the peer will send as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which are not IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.
- VTI and crypto map configurations can co-exist on the same physical interface, provided the peer address configured in the crypto map and the tunnel destination for the VTI are different.
- By default, all traffic through VTI is encrypted.
- By default, the security level for VTI interfaces is 0.
- Access list can be applied on a VTI interface to control traffic through VTI.
- Only BGP is supported over VTI.
- If ASA is terminating IOS IKEv2 VTI clients, disable the config-exchange request on IOS, because ASA cannot retrieve the mode-CFG attributes for this L2L session initiated by an IOS VTI client.
- IPv6 is not supported.

Related Information:

- Create a Site-to-Site VPN Tunnel Between ASAs, on page 255
- Encryption and Hash Algorithms Used in VPN
- Exempt Remote Access VPN Traffic from NAT, on page 308

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

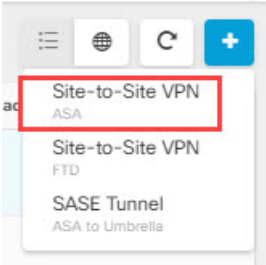
Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase. For IKEv1, you must configure the same preshared key on each peer. For IKEv2, you can configure unique keys on each peer.

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 Tunnel Between ASAs

Use the following procedure to create a site-to-site VPN tunnel between two ASAs or an ASA with an Extranet device:

Step 1 Click the blue plus on the top right corner and click **Site-to-Site VPN** with ASA label.



Step 2 In the **Configuration Name** field, enter a name for the site-to-site VPN configuration you create.

Step 3 Select one of the options to create a new **Policy Based** or **Route Based** site-to-site VPN.

Step 4 In the **Peer Devices** section, do the following:

a) **Peer 1**: Select an ASA device and then click **Select**.

b) **Peer 2**: Select the other ASA device and then click **Select**.

Extranet: If you want to choose an extranet device in Peer 2, click the Extranet slider to enable it.

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 the static interface or **DHCP Assigned** for the dynamic interface.

c) Click **Next**.
d) Choose the **VPN Access Interface** for the endpoint devices.
e) (Applicable to Route Based VPN) Choose the **LAN Interfaces** that controls the LAN subnet. You can select multiple interfaces.

The networks attached to the selected LAN interfaces will be added to the routing policy access list. The traffic matching the routing policy access list will be encrypted/decrypted by the VPN tunnel.

f) Click **Add Network** to add the **Protected Networks** for the participating devices. A protected network defines the networks that are protected by this VPN endpoint.
g) (Optional and applicable to Policy Based) 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 ASA Site-to-Site VPN Traffic from NAT.
h) Click **Next**.

Step 5 (Applicable to Route Based) In the **Tunnel Details**, the **VTI Address** fields are automatically filled once the peer devices are configured in the previous step. If necessary, you can manually enter an IP address that will be used as the new VTI.

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 About Global IKE Policies.

Based on the configuration made by the user, CDO suggests the IKE settings. You can either continue with the recommended IKE configuration settings or define a new one.

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 IKE versions as appropriate.

By default, **IKEV Version 2** is enabled.

Note Enabling both IKE versions is not allowed for route-based VPN.

b) Click **Add IKEv2 Policy** and select the IKEv2 policies

Note Click **Create New IKEv2 Policy** to create new IKEv2 policies. For more information about creating new IKEv2 policies, see Managing IKEv2 Policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the x icon.

c) Enter the **Pre-Shared Key** for the participating devices. Preshared keys are secret key strings configured on each peer in the connection. IKE uses these keys 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 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

d) Click **IKE Version 1** to enable it.

e) Click **Add IKEv1 Policy** and select the IKEv1 policies. Click **Create New IKEv1 Policy** to create new IKEv1 policies. For more information about creating new IKEv1 policies, see theManaging IKEv1 Policies. To delete an existing IKEv1 Policy, hover-over the selected policy and click the x icon.

f) (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.

g) Click **Next**.

Step 7 In the **IPSec Settings** section, based on the configuration made by the user, CDO suggests the IKEv2 proposals. You can either continue with the recommended IKE configuration settings or define a new one. For more information on the IPSec settings, see the Configuring IPsec Proposals.

a) Click **+ IKEv2 Proposals** to select the IPSec configuration. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the x icon.

Note Click **Create New IKEv2 Proposals** to create new IKEv2 proposals. For more information about creating new IKEv2 policies, see the About IPsec Proposals.

b) Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Encryption and Hash Algorithms Used in VPN, on page 252

c) Click **Next**.

Step 8 In the **Finish** section, read the configuration and continue further only if you're satisfied with your configuration, click **Submit**.

You are directed to the VPN Tunnels page that shows the newly configured site-to-site VPN tunnel. The changes are staged and must be deployed manually. A routing policy is created to route the VTI traffic automatically between the devices over the VTI tunnel. To see this policy, select the device from the **Inventory** page and choose **Configuration** > **Diff**.

See the Deploy Configuration Changes Made Using the CDO GUI section to deploy site-to-site VPN configuration on the devices associated with the new tunnel.

Exempt Site-to-Site VPN Traffic from NAT

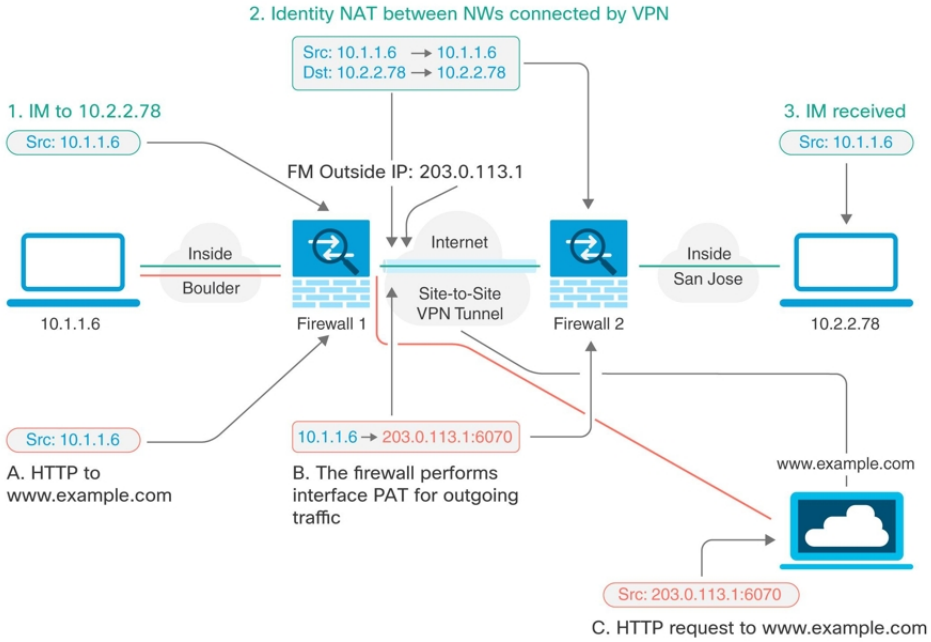
When you have a site-to-site VPN connection defined on an interface, and you also have NAT rules for that interface, you can optionally exempt the traffic on the VPN from the NAT rules. You might want to do this if the remote end of the VPN connection can handle your internal addresses.

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.

Step 1 Create objects to define the various networks.

a. Click the blue plus button to create an object.

b. Click **ASA** > **Network**.

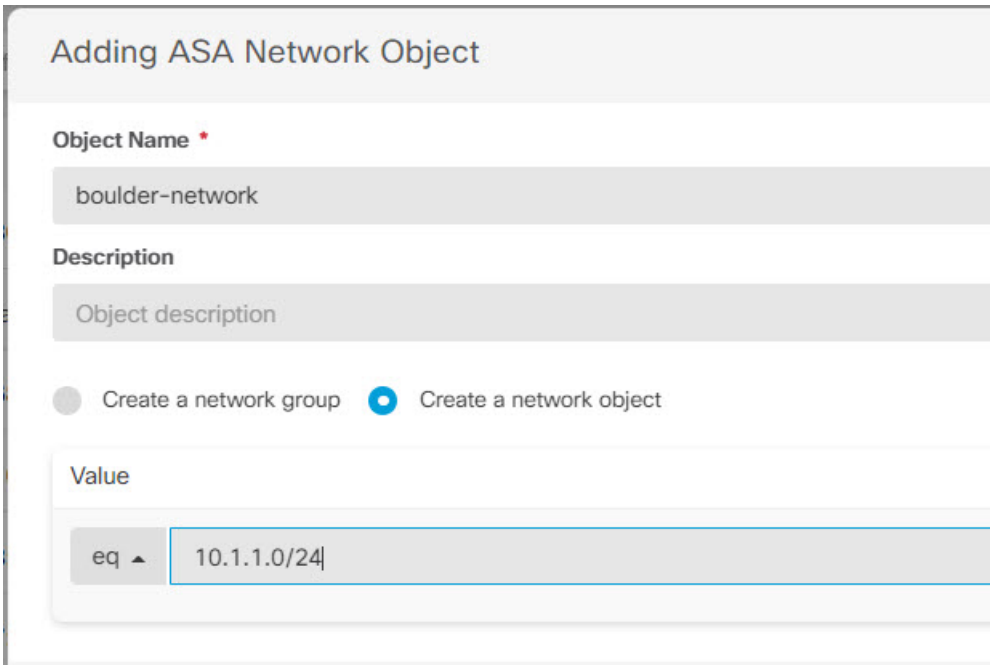
c. Identify the Boulder inside network.

d. Enter an object name (for example, boulder-network).

e. Select **Create a network object**.

f. 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.



g. Click **Add**.

h. Click the blue plus button to create an object.

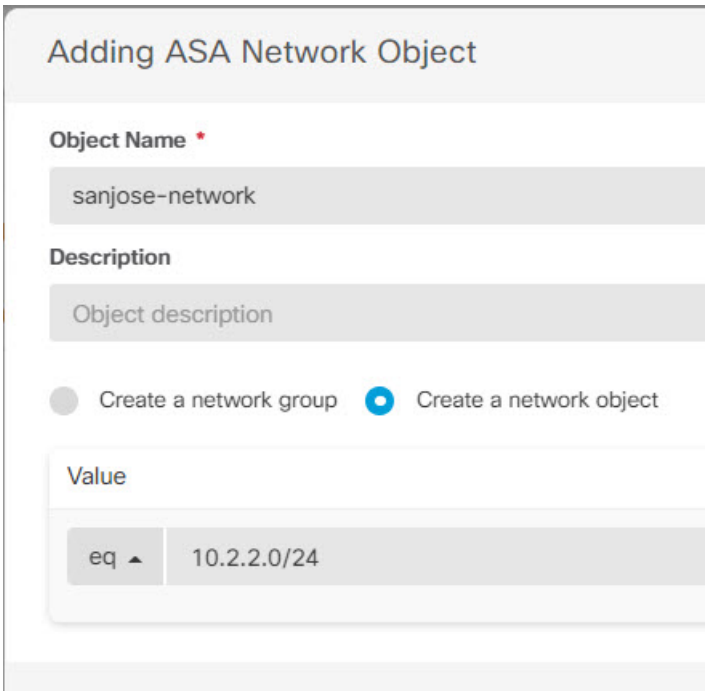
i. Define the inside San Jose network.

j. Enter the object name (for example, san-jose).

k. Select **Create a network object**.

l. 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.



m. Click **Add**.

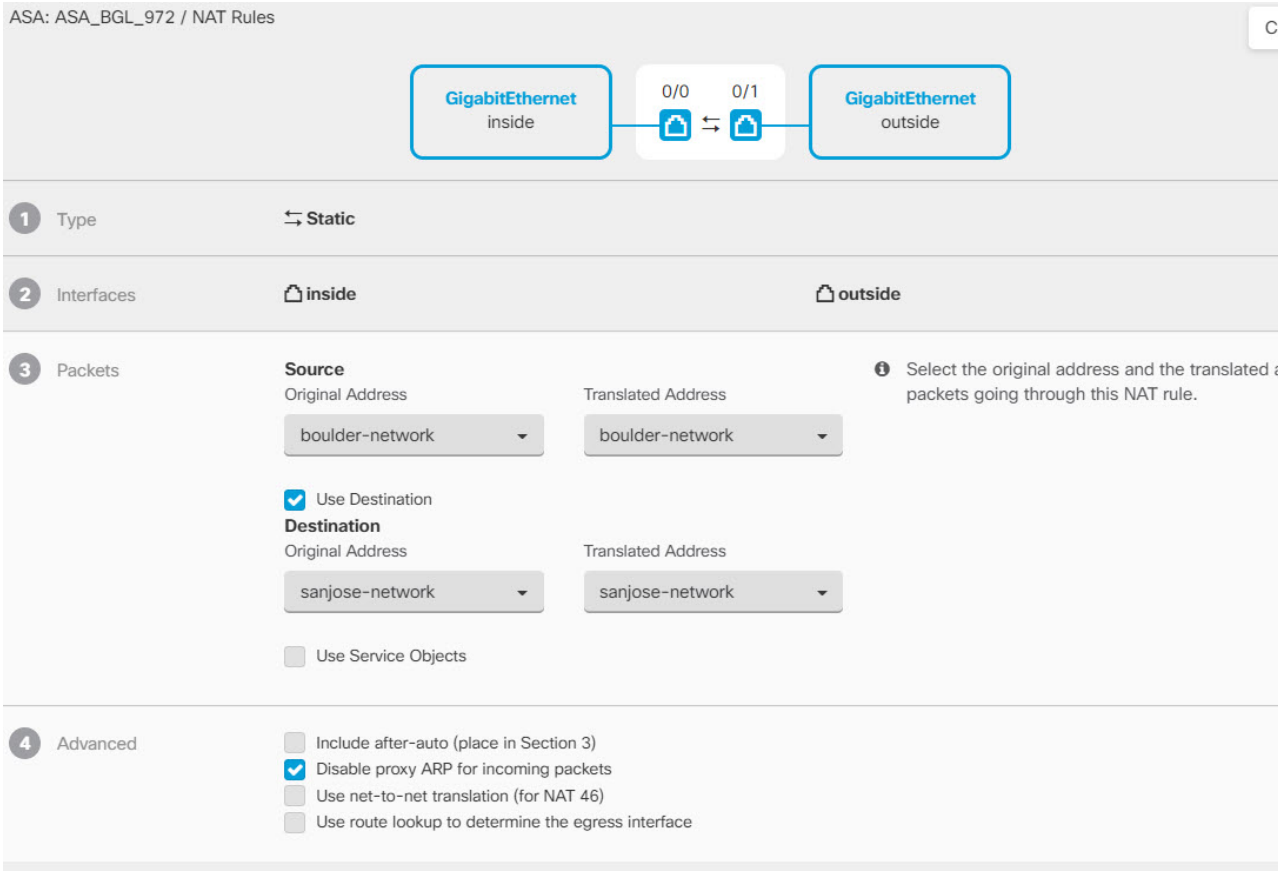
Step 2 Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

a. Use the filter to find the device for which you want to create the NAT rule.

b. In the Management area of the details panel, click **NAT** NAT.

c. 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.

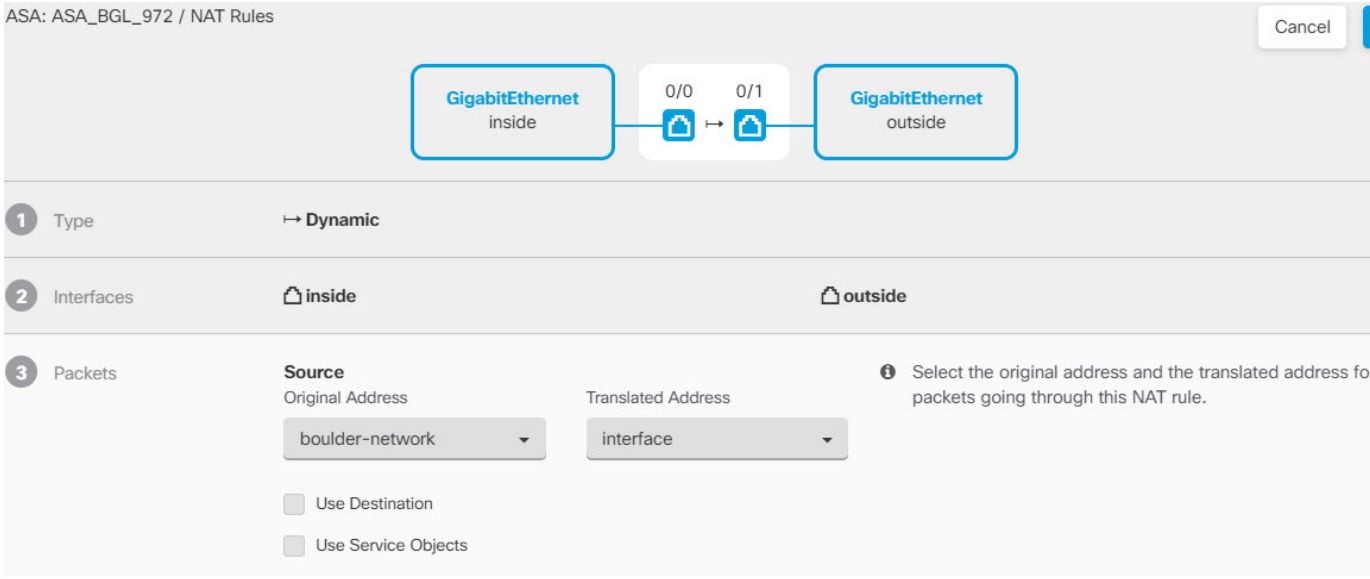
Step 3 Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder). **Note**: There might already be dynamic interface PAT rules for the inside interfaces, covering any IPv4 traffic, as these are created by default during initial configuration. 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 CDO. For more information, see Deploy Configuration Changes Made Using the CDO GUI, on page 236.

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."

Site-to-Site VPN Configuration Between ASA and Multicloud Defense Gateway

You can create site-to-site IPsec connections between an ASA and a Multicloud Defense Gateway that complies with all relevant standards. After the VPN connection is established, the hosts behind the firewall can connect to the hosts behind the gateway through the secure VPN tunnel.

Multicloud Defense currently supports Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle OCI cloud accounts.

Create a Site-to-Site VPN Between ASA and Multicloud Defense Gateway

Use the following procedure to create a VPN tunnel between an ASA device that is managed by CDO and Multicloud Defense Gateway from the CDO dashboard:

Before you begin

Ensure that the following prerequisites are met:

- The ASA device must not have any pending changes.
- Create a BGP profile in the ASA console prior to creating a VPN tunnel. See Configure ASA Border Gateway Protocol for more information.
- The Multicloud Defense Gateway must be in the **Active** state.
- The Multicloud Defense Gateway must be VPN enabled. See Enable VPN within the gateway.
- Read the ASA site-to-site VPN limitations and guidelines for more information.
- Read the Multicloud Defense Gateway prerequisites and limitations for more information.

Step 1 Click the create tunnel () button on the top-right corner and click **Site-to-Site VPN** with the **Multicloud Defense** label.

Step 2 In the **Configuration Name** field, enter a name enter a name for the site-to-site VPN configuration you create.

Step 3 In the peer devices area, provide the following information:

- **Device 1**: From the drop-down list, click the **ASA** tab and select the ASA device you want.
- **Device 2**: From the drop-down list, click the **Multicloud Defense** tab and select the gateway you want.
- **VPN Access Interface**: Select an ASA interface to be used for connecting to the Multicloud Defense.
- **Public IP (optional)**: Specify the public IP address of the NAT that maps to the outside interface of the selected ASA.
- **Routing** : Click **Add Networks** and select one or more protected networks from ASA to create a site-to-site tunnel between the selected networks and the Multicloud Defense Gateway.

Step 4 Click **Next**.

Step 5 In the **Tunnel Details** area, provide the following information:

- **Virtual Tunnel Interface IP**: Specify the addresses for the new **Virtual Tunnel Interfaces** on the peers. CDO provides a sample address for ASA which you can change if it causes conflict. You can assign any unused IP address that is currently not used on this device.
- **Autonomous System Number** (Peer 1): If the ASA device does not have an autonomous system number configured, CDO will suggest one for the device, which can be modified. If the device already has an autonomous system number configured, the current value will be displayed and cannot be modified.
- **Autonomous System Number** (Peer 2): If a BGP profile is assigned to the Multicloud Defense Gateway, the autonomous number associated with the profile is displayed, which cannot be modified. See Add a Multicloud Defense Gateway.

Step 6 Click **Next**.

Step 7 In the **IKE Settings** area, CDO generates a default **Pre-Shared Key**. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.

Step 8 Click **Next**.

Step 9 In the **Finish** area, review the configuration and continue further only if you're satisfied with the configuration.

By default, the **Deploy changes to ASA immediately** check box is checked to deploy the configurations immediately to the ASA device after clicking **Submit**.

If you want to review and deploy the configurations manually later, then uncheck this check box.

Step 10 Click **Submit**.

The configurations are pushed to the Multicloud Defense Gateway.

The VPN page in CDO shows the site-to-site tunnel created between the peers. You will be able to see the corresponding tunnel in the Multicloud Defense Gateway portal.

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 265

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.

Step 1 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 2 Enter an **object name**, up to 128 characters.

Step 3 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 4 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 266

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.

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 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, Cisco Defense Orchestrator 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 268

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,Cisco Defense Orchestrator 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.

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 270

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.

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 ASA Site-to-Site Virtual Private Networks

CDO allows you to monitor already existing site-to-site VPN configurations on onboarded ASA devices. It doesn't allow you to modify or delete the site-to-site configuration.

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

- CDO runs this connectivity check command on the ASA 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:

Step 1 From the main navigation bar, click VPN > ASA/FDM Site-to-Site VPN.

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

CDO provides a consolidated information about site-to-site VPN connections created in the tenant.

In the left pane, click **Dashboard**. 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

CDO can identify VPN issues on ASA. (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 273

Find VPN Tunnels with Missing Peers

The "Missing IP Peer" condition is more likely to occur on ASA devices than FDM-managed devices.

Step 1 In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** 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. CDO 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

Step 1 In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** 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.

Step 1 In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** 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.

Step 1 In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** 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.

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

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 233.

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.

Step 1 From the main navigation bar, navigate **VPN > ASA/FDM Site-to-Site VPN**.

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** - CDO 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 CDO or not managed (unmanaged) by CDO.
  - **Managed** – Filter by devices that CDO manages.
  - **Unmanaged** – Filter by devices that CDO 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

CDO will discover a site-to-site VPN tunnel when one of the peers is onboarded. If the second peer is not managed by CDO, you can filter the list of VPN tunnels to find the unmanaged device and onboard it:

Step 1 In the main navigation bar, select **VPN** > **ASA/FDM Site-to-Site VPN** 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 127
- Onboard ASA Device to CDO, on page 127

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.

Step 1 In the left pane, click **VPN > ASA/FDM Site-to-Site VPN**.

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

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 CDO. 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 CDO 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 CDO 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:

Step 1 In the left pane, click **VPN > ASA/FDM Site-to-Site VPN.**

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

Step 1 In the left pane, click **VPN > ASA/FDM Site-to-Site VPN.**

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 CDO 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 CDO Connectivity status shows **active**, the AWS tunnel state is **Up**. If the CDO 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 CDO Site-To-Site VPN Tunnel

Step 1 In the left pane, choose **VPN**> **Site-to-Site VPN**.

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:

- Configure Remote Access Virtual Private Network for ASA, on page 277

Configure Remote Access Virtual Private Network for ASA

The ASA creates a remote access virtual private network (VPN) by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. It can create single-user-to-LAN connections and LAN-to-LAN connections.

The secure connection is called a tunnel, and the ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination.

CDO provides an intuitive user interface for configuring a new remote access Virtual Private Network. It also allows you to quickly and easily configure remote access VPN connection for multiple Adaptive Security Appliance (ASA) devices onboarded in CDO.

CDO allows you to configure the remote access VPN configuration on ASA devices from scratch. It also allows you to manage the remote access VPN settings that have already been configured using another ASA management tool, such as the Adaptive Security Defense Manager (ASDM) or Cisco Security Manager (CSM). When you onboard an ASA device that already has remote access VPN settings, CDO automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. This default configuration can contain all the connection profile objects that are defined on the device. If you want to understand the RAVPN attributes that are read into CDO, see the Manage and Deploy Pre-existing ASA Remote Access VPN Configuration section. Otherwise, you can start performing steps described in the "End-to-End Remote Access VPN Configuration Process for ASA" section.

Related Information:

- End-to-End Remote Access VPN Configuration Process for ASA
  - Configure Identity Sources for ASA
    - Create an ASA Active Directory Realm Object
    - Create an ASA RADIUS Server Object or Group
  - Create ASA Remote Access VPN Group Policies, on page 284
  - Create ASA Remote Access VPN Configuration, on page 290
  - Configure ASA Remote Access VPN Connection Profile, on page 294

- Manage and Deploy Pre-existing ASA Remote Access VPN Configuration
- Create IP Address Pool
- Exempt Remote Access VPN Traffic from NAT, on page 308
- Verify ASA Remote Access VPN Configuration
- View ASA Remote Access VPN Configuration Details

End-to-End Remote Access VPN Configuration Process for ASA

This section provides the end-to-end procedure for configuring remote access VPN on an ASA device onboarded to CDO.

To enable remote access VPN for your clients, you need to configure several separate items. The following procedure provides the end-to-end process.

Step 1 Configure the identity source used for authenticating remote users. See Configure Identity Sources for ASA for more information.

You can use the following sources to authenticate users attempting to connect to your network using remote access 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 an ASA Active Directory Realm Object.
- RADIUS server group: As a primary or secondary authentication source, and for authorization and accounting. See Create an ASA 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 ASA device only from the Adaptive Security Device Manager (ASDM). See the "Configure Local User Groups" section in the Objects for Access Control" chapter of the Cisco ASA Series Firewall ASDM Configuration Guide, X.Y.

Step 2 (optional) Create ASA Remote Access VPN Group Policies, on page 284. 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 3 Create ASA Remote Access VPN Configuration, on page 290.

Step 4 Configure ASA Remote Access VPN Connection Profile, on page 294.

Step 5 (optional) Exempt Remote Access VPN Traffic from NAT, on page 308.

Step 6 Deploy Configuration Changes from CDO to ASA.

Important If you change the Remote Access VPN configuration by using a local manager like Adaptive Security Device Manager (ASDM), the **Configuration Status** of that device in CDO shows "Conflict Detected". See Out-of-Band Changes on Devices. You can Resolve Configuration Conflicts on this ASA.

What to do next

Next Steps

Once the remote access VPN configuration is downloaded to the ASA 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 VPN sessions from all onboarded ASA remote access VPN head-ends in your tenant. See Monitor Remote Access Virtual Private Network Sessions.

Configure Identity Sources for ASA

Identity sources, such as Microsoft Active Directory (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 CDO.

Click **Objects** > **ASA Objects**, then click ( )>**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.

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 Active Directory 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 distinguished name. 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 Active Directory 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:

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 an ASA 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 an ASA RADIUS Server Object or Group for more information.

Create an ASA Active Directory Realm Object

When you create or edit an identity source object such as an AD realm object, CDO sends the configuration request to the ASA devices through the SDC. The ASA then communicates with the configured AD realm.

Use the following procedure to create an object:

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click **Create Object** (+)**RA VPN Objects (ASA & FDM)** > **Identity Source**.

Step 3 Enter an **Object Name** for the object.

Step 4 Select the **Device Type** as **ASA**.

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 Active Directory, 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.

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 **LDAPS** to use SSL to secure communications between the ASA and the LDAP server. It requires LDAP over SSL. Use port 636.

  The default is **None**, which means that user and group information is downloaded in clear text.

Step 8 (Optional) Use the **Test** button to validate the configuration.

Step 9 (Optional) Click **Add another configuration** to add multiple Active Directory (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**.

Edit an ASA 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.

Step 1 In the left pane, click **Objects > ASA 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 CDO 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 Deploy Configuration Changes from CDO to ASA now the changes you made, or wait and deploy multiple changes at once.

Create an ASA RADIUS Server Object or Group

When you create or edit an identity source object such as a RADIUS server object or a group of RADIUS server objects, CDO sends the configuration request to ASA devices through the SDC.

Create an ASA RADIUS Server Object

RADIUS servers provide AAA (authentication, authorization, and accounting) services.

Use the following procedure to create an object:

Step 1 In the CDO navigation bar on the left, click **Objects > ASA Objects**.

Step 2 Click **Create Object** ()**> RA VPN Objects (ASA & FDM)** > **Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 Select the **Device Type** as **ASA**.

Step 5 Select **RADIUS Server** as the **Identity Source Type**. 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 ASA 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 Click **Add**.

Step 8 Deploy Configuration Changes from CDO to ASA now the changes you made, or wait and deploy multiple changes at once.

Create an ASA 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:

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click **Create Object** ( ) **RA VPN Objects (ASA & FDM) Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 Select the **Device Type** as **ASA**.

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 **RADIUS SERVER 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. ASA then defaults to the next server in the list.

Step 9 Deploy Configuration Changes from CDO to ASA now the changes you made, or wait and deploy multiple changes at once.

Edit an ASA Radius Server Object or Group

Use the following procedure to edit a Radius server object or Radius server group:

Step 1 In the left pane, click **Objects > ASA 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 CDO 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 Deploy Configuration Changes from CDO to ASA now the changes you made, or wait and deploy multiple changes at once.

Create ASA Remote Access 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 remote access VPN configuration. Resolve all inconsistencies before adding the group policy to the remote access VPN Configuration.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **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 **ASA**.

Step 6 Do any of the following:

- Click the required tabs and configure the attributes on the page:
  - ASA Remote Access VPN Group Policy Attributes
  - AnyConnect Client Profiles, on page 285
  - Session Setting Attributes, on page 286
  - Address Assignment Attributes, on page 286
  - Split Tunneling Attributes, on page 287
  - AnyConnect Attributes, on page 288
  - Traffic Filters Attributes, on page 289
  - Windows Browser Proxy Attributes, on page 290

Step 7 Click **Save** to create the group policy.

ASA Remote Access VPN Group Policy Attributes

The section describes the attributes associated with the ASA remote access VPN group policy.

General Attributes

The general attributes of a group policy define the name of the group and some other basic settings.

- **DNS Server**: Enter the IP address(s) of DNS servers for domain name resolution when connected to the VPN. You can separate the addresses using a comma.
- **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 remote access 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

This feature is supported on FTD 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 310. 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 the IP address pool 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. To create a new Create IP Address Pool. 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. **Note**: You can configure both IPv4 and IPv6 address pools for the same group policy. If both versions of IP addresses are configured in the same group policy, clients configured for IPv4 will get an IPv4 address, clients configured for IPv6 will get an IPv6 address, and clients configured for both IPv4 and IPv6 addresses will get both an IPv4 and an IPv6 address.

- **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, enter the network object that contains the network number host address. For example, to tell the DHCP server to use addresses from the 192.168.5.0/24 subnet pool, enter 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).

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 remote access 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 FTD devices and increases the bandwidth on the outside interface.

Before you begin

For creating a split tunnel policy for IPv4 networks and another for IPv6 networks, the access-list you specify is used for both protocols. So, the access-list should contain access control entries (ACEs) for both IPv4 and IPv6 traffic.

When an ASA device is onboarded to CDO, it reads the extended ACLs associated with the device. See Group Policy for more information. If you want to create new ACLs, see Create an ASA Access List to create them.

Note Ensure that you specify the network intended for split tunneling as the source network in the ACL you are creating.

- **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 remote access 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 extended access list that defines the source network. Any traffic from these sources goes through the protected tunnel. The client routes traffic from any other source to connections outside the tunnel (such as a local Wi-Fi or network connection).

- **Exclude networks specified below**: Select the network objects that define the source network. The client routes any traffic from these sources to connections outside the tunnel. Traffic from any other source goes through the tunnel.
- **Network List**: Select the extended ACL network that can have both IPv4 and IPv6 networks.

- **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 remote access VPN users to specific resources, based on host or subnet address and protocol, or VLAN. By default, remote access 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 FDM, 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 ASA Remote Access VPN Configuration

CDO allows you to add one or more Adaptive Security Appliance (ASA) devices to the remote access VPN configuration wizard and configure the VPN interfaces, access control, and NAT exemption settings associated with the devices. Therefore, each remote access VPN configuration can have connection profiles and group policies shared across multiple ASA devices that are associated with the remote access VPN configuration. Further, you can enhance the configuration by creating connection profiles and group policies.

You can either onboard an ASA device that has already been configured with remote access VPN settings or a new device without remote access VPN settings. See Onboard ASA Device to CDO, on page 127. When you onboard an ASA device that already has remote access VPN settings, CDO automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. Also, this default configuration can contain all the connection profile objects that are defined on the device. See Manage and Deploy Pre-existing ASA Remote Access VPN Configuration for more information. CDO allows you to delete the default configuration.

Important

- You are not allowed to add ASA and FTD in the same Remote Access VPN Configuration.
- An ASA device cannot have more than one remote access VPN Configuration.

Before you begin

Before adding the ASA device to the remote access VPN configuration, the following prerequisites must be met on the ASA device:

- License requirements.

  Device must be enabled for export-controlled functionality.

  To view the license summary of your ASA device, execute the show license summary command in the ASA command-line interface. To use the CDO ASA CLI interface, see CDO Command Line Interface.

  - Example of export-controlled functionality enabled in the license summary :

```
Registration: Status: REGISTERED Smart Account: Cisco SVS temp-request access
licensing@cisco.com Export-Controlled Functionality: ALLOWED

Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

  The 'Export-Controlled Functionality' property must be in the 'Allowed' state for creating or editing the VPN configuration.

  If this property is in the 'Not Allowed' state, CDO displays an error message ('remote access VPN cannot be configured for devices which are not export compliant.') when you are creating or modifying the VPN configuration and doesn't allow remote access VPN configuration on the device.

- Device Identity Certificates.

  Certificates are required to authenticate connections between the clients and the ASA device. Before starting the VPN configuration, ensure that the identity certificate is already present on the ASA device.

  To determine whether or not the certificate is present on the device, execute the **show crypto CA Certificates** command in the ASA command-line interface. To use the CDO ASA CLI interface, see CDO Command Line Interface.

  If the identity certificate is not present or you want to enroll in a new certificate, install them on ASA using CDO. See ASA Certificate Management.

  The usage of digital certificates in remote access VPN context is explained in Remote Access VPN Certificate-Based Authentication, on page 307.

- Outside interfaces.

  The outside interfaces must be configured already on the ASA device. **You need to use either ASDM or ASA CLI to configure interfaces**. To know configure interfaces using ASDM, see the "Interfaces" book of the Cisco ASA Series General Operations CLI Configuration Guide, X.Y.

- Download the AnyConnect packages and upload them to a remote server. Later, use the remote access VPN wizard or ASA File Management wizard to upload the AnyConnect software packages from the server to ASAs. See Manage AnyConnect Software Packages on ASA Devices for instructions.

- There are no configuration deployments pending.
- If you are using the local database for authentication Add user accounts to the local database using ASDM or ASA CLI.

  To add user accounts using ASDM, see the "Add a User Account to the Local Database" section in the "AAA Servers and the Local Database" book of the Cisco ASA Series VPN CLI Configuration Guide, X.Y.

  To add user accounts using ASA CLI, execute **username[***username***] password [***password***] privilege [***priv_level]* command.
- ASA changes are synchronized to CDO.
  1. In the left pane, click **Inventory** and search for one or more ASA devices to be synchronized.
  2. Select one or more devices and then click **Check for changes**. CDO communicates with one or more FTD devices to synchronize the changes.
- Remote access VPN configuration group policy objects are consistent.
  - Ensure that all inconsistent group policy objects are resolved as they cannot be added to the remote access 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.

Step 1 Onboard ASA Device to CDO, on page 127.

Step 2 In the left pane, click **VPN** > **ASA/FDM Remote Access VPN Configuration**.

Step 3 Click the blue plus  button to create a new remote access VPN configuration.

Step 4 Enter a name for the Remote Access VPN configuration.

Step 5 Click the blue plus  button to add ASA 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 ASA device that you want to add and click **Select**. **Important**: You are not allowed to add ASA and FTD 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.
- **Outside Interface**: Select 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.

  Attention You cannot create or modify remote access VPN configuration for devices that are not export compliant. You must license the ASA device with export-controlled functionality enabled and try again.

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**: NAT exemption exempts addresses from translation and allows both translated and remote hosts to initiate connections with your protected hosts. Configure NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. See Exempt Remote Access VPN Traffic from NAT, on page 308.

c. Click **OK**.

The **AnyConnect Packages Detected** shows the AnyConnect packages that are already available on the device.

There are two options to upload AnyConnect package to ASA from remote access VPN wizard:

- (Option 1): Select a package from CDO's repository. The ASA must have access to the internet.
- (Option 2): Specify the ftp/http/https/scp/smb/tftp URL location where the AnyConnect package is preloaded.

See Manage AnyConnect Software Packages on ASA Devices for instructions.

Note Note: If you want to replace an existing package, see Manage AnyConnect Software Packages on ASA Devices.

Step 6 Click **OK**.

The ASA VPN configuration is created.

Modify ASA Remote Access VPN Configuration

You can modify the name and the device details of an existing remote access VPN configuration.

Step 1 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 ASA device.
  - Click **Edit** to modify the existing remote access VPN configuration.
  - Click **Remove** to remove the ASA device from the remote access VPN configuration. All connection profiles and remote access 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 ASA if that is the only device using the configuration. Alternatively, you can remove the remote access VPN configuration.

Step 2 Deploy Configuration Changes from CDO to ASA.

What to do next

You can also search for remote access VPN configuration by typing the name of the configuration or device.
Related Information:

- Configure ASA Remote Access VPN Connection Profile, on page 294.

Configure ASA Remote Access VPN Connection Profile

A Remote Access 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 pools for assigning users IP addresses, and the group policies that define various user-oriented attributes.

You can create multiple profiles within the remote access 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.

A remote access 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

Create ASA Remote Access VPN Configuration, on page 290.

Step 1 In the left pane, click **VPN** > **ASA/FDM Remote Access VPN Configuration**. You can click a VPN configuration to view the summary information on how many connection profiles and group policies are currently configured.

Note To know the group policies assigned to the device, in **Actions**, click **Group Policies**. Group Policies assigned to connection profiles are automatically added to the list and cannot be removed.

If the group policy you need does not yet exist, click  and select from the list. You can create additional group policies to provide the services you require. See Create ASA Remote Access VPN Group Policies, on page 284.

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 ASA 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 , on page 296.
- **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. See Create ASA Remote Access VPN Group Policies, on page 284.

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**.

Step 11 Perform step 5 of End-to-End Remote Access VPN Configuration Process for ASA.

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**: Authentication provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted. 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.
  - A RADIUS server group.
  - LocalIdentitySource (the local user database): You can define users directly on the device and not use an external server.

    You can click Configure Identity Sources for ASA to create new identity sources.
- **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 the 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.

  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.

  You can click Create an ASA RADIUS Server Object or Group to create new server groups.
- **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 ASA 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.

  You can click Create an ASA RADIUS Server Object or Group to create new server groups.

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 ASA Remote Access VPN Connection Profile, on page 294.

The 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. To create new IPv4 or IPV6 address pools, see Create IP Address Pool.
- **DHCP Servers**: First, configure a DHCP server with one or more IPv4 address ranges for the remote access 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 Create ASA Remote Access VPN Group Policies 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.

Related Information:

End-to-End Remote Access VPN Configuration Process for ASA

Manage AnyConnect Software Packages on ASA Devices

You can perform one of the following steps to upload an AnyConnect package using the remote access VPN wizard:

- Upload the package from the CDO repository.
- Upload the package from the server using HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

Upload an AnyConnect Package from CDO Repository

The remote access VPN Configuration wizard presents AnyConnect packages per operating system from the CDO 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.

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.

Upload an AnyConnect Package to ASA from Server

Download the AnyConnect client software packages to your computer and upload them to a remote server accessible from ASAs. Later, use the RA VPN wizard or ASA File Management wizard to upload the AnyConnect software packages from that server to ASAs. DNS must be configured correctly on the device for URLs that use a domain name.

The ASA RA VPN wizard supports uploading packages using HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazon/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://root:cisco123@10.10.16.6//root/events_send.py

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.

Important If you choose to upload the package using the ASA File Management wizard, do not modify the package's name after downloading them.

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.

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 server. Ensure that there is a network route from the ASA device and the server.

The ASA RA VPN wizard supports uploading packages HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

Important 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 ASA device.
- 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, you can download the file 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 to ASA

You can either use the remote access VPN wizard or ASA File Management wizard to upload the AnyConnect software packages to ASAs.

Use the following procedure to upload new AnyConnect packages to an ASA device from an HTTP or HTTPS server:

Step 1 In the **AnyConnect Package Detected**, you can upload separate packages for Windows, Mac, and Linux endpoints.

Step 2 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 3 Click to upload the package. CDO 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 ASA devices to the remote access VPN configuration, you can upload the AnyConnect packages to them.

Step 4 Click **OK**. The AnyConnect packages are added to the remote access VPN configuration.

Step 5 Continue to Create ASA Remote Access VPN Configuration from step 5 onwards.

What to do next

To complete a VPN connection, your users must install the AnyConnect client software on their workstation. For more information, see Install the AnyConnect Client Software on ASA .

Upload AnyConnect Packages using File Management Wizard

Use the File Management wizard to upload AnyConnect packages to a single or multiple ASA devices from an HTTP, HTTPS, TFTP, FTP, SMB, or SCP server. When you want to push AnyConnect packages to multiple ASA devices simultaneously, the bulk upload comes in handy. For more information, see ASA File Management.

Important If you choose to upload the package using the ASA File Management wizard, do not modify the package's name after downloading them.

Once the upload is complete, open the ASA RA VPN Configuration wizard and notice that the packages are auto-detected. If you upload multiple packages for an OS version, the wizard lists them in a drop-down allowing you to select one among them. Then, you can create the RA VPN configuration and deploy them to the devices.

Replace an AnyConnect Package

If the AnyConnect packages are already present on the devices, you can see them in the remote access 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 ASA can reach.

Step 1 In the left pane, click **VPN** > **ASA/FDM Remote Access VPN**.

Step 2 Select the remote access 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 remote access VPN configuration.

Step 6 Continue to Create ASA Remote Access VPN Configuration, on page 290 from step 6 onwards.

Delete an AnyConnect Package

Step 1 In the left pane, click **VPN** > **ASA/FDM Remote Access VPN**.

Step 2 Select the remote access 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 Deploy Configuration Changes from CDO to ASA.

Manage and Deploy Pre-existing ASA Remote Access VPN Configuration

When you onboard an ASDM managed ASA device that already has remote access VPN settings, it discovers and displays the existing remote access VPN configurations. CDO automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. There are some remote access VPN configurations that aren't read or supported in the CDO but can be configured in the CDO command-line interface.

Note This section doesn't cover every supported or unsupported configuration in CDO. Instead, it only describes the most commonly used ones.

To see the remote access VPN configurations from an onboarded ASA, perform the following steps:

Step 1 In the left pane, click **VPN** > **ASA/FDM Remote Access VPN Configuration**.

Step 2 Click the remote access VPN configuration corresponding to the onboarded ASA device. CDO automatically creates a "**Default_RA_VPN_Configuration**" and associates the ASA device with this configuration. You can delete the default configuration. The ASA remote access VPN configurations that are read in CDO are classified as follows:

- Device settings

- Connection profiles
- Group policies

Device Settings

The RA VPN configurations associated with the onboarded ASA device appear in **Default_RA_VPN_Configuration**. You need to click on this configuration to see the name of the ASA device (in the **Devices** pane on the right) associated with that configuration. You can also see the AnyConnect packages present in the ASA devices by clicking the edit button.

Connection Profile

CDO supports and reads the connection profiles defined in "AnyConnect Client VPN Access" of the ASA device. It does not support the "Clientless SSL VPN Access" configuration.

To see the connection profile attributes, perform the following:

Step 1 Expand **Default_RA_VPN_Configuration**.

Step 2 Click one of the connection profiles that you want and click **Edit**.

All the basic and advanced ASA RA VPN attributes can be seen in the **Connection Profile name and details** of the CDO RA VPN configuration page.

Note You can delete the default configuration (Select the default RA VPN configuration and in the **Actions** pane on the right, click **Remove**).

Primary Identity Source

- CDO reads the **Connection Aliases** and **Group URLs** attributes as **Group Alias** and **Group URL**.

Note

- The connection profiles configured with SAML, Multiple certificates and AAA, and Multiple certificates aren't read.
- The authentication server group with the interface and server group is not supported.

- CDO supports the AnyConnect connection profiles configured with "AAA", "AAA and certificate", and "Certificate only" authentication methods in **Primary Identity Source**.
- The **AAA Server Group** is read in CDO as **Primary Identity Source for User Authentication** in**Primary Identity Source** (You can see this attribute by selecting **AAA** or **AAA and Client Certificate** as the **Authentication Type**).

- If the **AAA Server Group** has been configured something other than LOCAL, CDO reads and displays this attribute in the **Fallback Local Identity Source** field under **Primary Identity Source**. (You can see this attribute by selecting **AAA** as the authentication type).

  To learn more about the server group attributes read in CDO, see AAA Server Groups.

Secondary Identity Source

The **Secondary Identity Source** displays the secondary authentication attributes of the ASA device. To see these attributes, select **AAA** or **AAA and Client Certificate** as the authentication type, and click **View Secondary Identity Source**.

- The **Secondary Identity Source for User Authentication** displays the secondary authentication **Server Group** attribute.
  - If the **Server Group** has been configured something other than LOCAL, CDO reads and displays this attribute in the **Fallback Local Identity Source for Secondary**field under **Secondary Identity Source**.
- CDO doesn't support the **Attribute Server** and **Interface-Specific Authorization Server Groups** attributes.

To learn more about the server group attributes read in CDO, see AAA Server Groups.

Authorization Server

- The **Authorization Server** displays the authorization **Server Group** attribute.
- CDO doesn't support the authorization server group with interface and server group.

To learn more about the RADIUS server group attributes read in CDO, see RADIUS Server Group.

Accounting Server

The **Accounting Server** displays the accounting **Server Group** attribute. To learn more about the server group attributes read in CDO, see RADIUS Server Group.

Client Address Pool Assignment

CDO reads the **Client Address Assignment attributes** (**DHCP Servers**, **Client Address Pools**, and **Client IPv6 Address Pools**) as objects. (You can see these attributes in **Client Address Pool Assignment**). The DHCP server details are read as literals.

Note CDO doesn't support the IP address pools assigned on specific interfaces. However, these attributes can be seen in the ASA command-line interface (CLI).

AAA Server Groups

CDO represents an LDAP Server Group and its associated LDAP Servers as an **Active Directory Realm** object. For Active Directory (AD), a realm is equivalent to an Active Directory domain. Note that CDO does read the AD password for AD realm objects that are already present.

Step 1 In the CDO navigation bar on the left, click **Objects > ASA Objects**.

Step 2 Apply the **Active Directory Realms**filter to see this object.

Step 3 Select the Active Directory Realm object that you want and click **Edit** to see its details.

What to do next

You can see that the AD realm contains the associated AD server and its configuration. If there are multiple Active Directory (AD) servers for 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. CDO displays a warning message in the Active Directory Realm object if these properties aren't the same. You have to correct these properties to make them consistent across the AD servers. If you continue without addressing this warning, CDO uses one of the AD server properties and applies it to other servers in that realm object.

RADIUS Server Group

The AAA RADIUS Server Group attributes of the ASA device are read in CDO as RADIUS Server Group objects.

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Apply the **RADIUS Server Group** filter to see this object.

Step 3 Select the object that you want and then click **Edit** to see its details.

- The **Enable dynamic authorization** in ASA is read in CDO as **Dynamic Authorization (for RA VPN only)**.
- The **Depletion** option in **Reactivation Mode** is read in CDO, and therefore the **Dead Time** value associated with depletion time is read in CDO. However, the **Timed** attribute is not read in CDO.
- CDO doesn't support **Accounting Mode**, **Timed**, **Enable interim accounting update**, **Enable interim accounting update**, and **Use authorization only mode**.

RADIUS Server

When CDO reads the Radius Servers from ASA, it creates a Radius server object specifies the name as "Name of the Radius server group_server name or IP address".

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Apply the **RADIUS Server** filter to see this object.

Step 3 Select the object that you want and then click **Edit** to see its details.

Group Policy

In the **Group Policy** section, click the drop-down to view the group policies associated with the device.

Attention CDO reads the group policies configured with tunneling protocol as **SSL VPN Client**.

CDO reads most of the group policy attributes configured in ASA. The information is displayed across the tabs in the RA VPN Group policy wizard. To see the details of group policies read from the ASA device, you need to perform the following:

Step 1 In the left pane, click **Objects > FTD Network Objects**.

Step 2 Filter for **RA VPN Group Policy**.

Step 3 Select the group policy associated with that device and click **Edit**.

What to do next

Note CDO doesn't support the Standard Access Control Lists (ACL) defined in the split tunneling in the ASA device. It supports the Extended Access Control Lists (ACL) and reads them as ACLs in the ASA policies. For more information, see ASA Remote Access VPN Group Policy Attributes. To see the policies, on the navigation bar, you can click **Policies** > **ASA Access Policies**.

To select the extended ACLs, perform the following:

- Click the **Split Tunneling** tab.
- Based on whether the traffic in ASA uses IPv4 or IPv6 addresses, select "Allow specified traffic over tunnel" or "Exclude networks specified below" from the corresponding drop-down list. Select the extended ACLs that are imported from ASA.

Create IP Address Pool

You can configure IPv4 and IPv6 IP address pools for ASAs to assign them to clients connecting remotely to your network using a VPN connection. The order in which you specify the pools is important. If you configure more than one address pool for a connection profile or group policy, the ASA uses them in the order in which you added them to the ASA.

To define the IPv4 address pool, provide the IP address range. An example of an IPv4 address pool is 10.10.147.100 - 10.10.147.177.

To define the IPv6 address pool, provide a starting IP address range, the address prefix, and the number of addresses configurable in the pool. An example of an IPv6 address pool is 2001:DB8:1::1.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Perform the following to create an IP address pool:

Step 1 In the left pane, click **Objects > ASA Objects**.

Step 2 Click the blue plus button and select **ASA** > **Address Pool**.

Step 3 In the **Create IP Address Pool** dialog box enter this information:

- **Object Name**: Enter the name of the address pool. It can be up to 64 characters
- **IPv4 address pool**: Select this radio button to configure IPv4 address pools.
  - **IPv4 Address Range**: Enter the first IP address and last IP address available in each configured pool. For example, 10.10.147.100 - 10.10.147.177.
  - **Mask**: Identifies the subnet on which this IP address pool resides.
- **IPv6 address pool**: Select this radio button to configure IPv6 address pools.
  - **IPv6 Address**: Enter the first IP address available in the configured pool and prefix length in bits in <address>/<prefix> format. For example, 2001:DB8:1::1/3.
  - **Number of Addresses**: Identifies the number of IPv6 addresses, starting at the IP Address, that are in the pool.

Step 4 Click **Save**.

Remote Access VPN Certificate-Based Authentication

The remote access VPN uses digital certificates for authenticating secure gateways and AnyConnect clients (endpoints) in the following scenarios:

Important CDO handles the installation of digital certificates on the VPN headends (ASA). It does not handle the installation of certificates on the AnyConnect client device. The administrator of your organization must handle it.

- Identify and authenticate the VPN headend device (ASA):

  VPN headends require an identity certificate to identify and authenticate themselves when the AnyConnect client requests a VPN connection. Using CDO, you must install the identity certificate on the device. See Installing an Identity Certificate Using PKCS12 or Certificate And Key. It is not mandatory to install the issuer's CA certificate on the AnyConnect client.

  While creating the Remote Access VPN configuration from CDO, assign the enrolled identity certificate to the outside interface of the device and download the configuration to the device. The identity certificate becomes fully operational on the outside interface of the device.

  When the AnyConnect client attempts to connect to VPN, the device authenticates itself by presenting its identity certificate to the AnyConnect client. The AnyConnect client verifies this identity certificate with its trusted CA certificate and trusts the certificate and thereby the device. If the CA certificate isn't installed on the AnyConnect client, the user must manually trust the device when prompted.

- Identify and authenticate the AnyConnect client:

Note This applies when you use "Client Certificate Only" or "AAA and Client Certificate" as the authentication method in the connection profile of remote access VPN configuration. It does not apply for "AAA Only".

Once the device is trusted, the AnyConnect client needs to authenticate itself to complete the VPN connection. You must install an identity certificate on the AnyConnect client and using CDO, install a trusted CA certificate on the device. These certificates must be issued from the same certificate authority. See Installing Trusted CA Certificate in ASA.

The AnyConnect client presents its identity certificate and the device verifies this certificate with its trusted CA certificate and establishes the VPN connection.

Exempt Remote Access VPN Traffic from NAT

Configure 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 remote access 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.

Before you begin

Create ASA network objects that match the configuration of the local IP address pools used in the connection profile and group policy of that device. These network objects must be assigned as the destination address and translated address when configuring the NAT rule. See Create an ASA Network Object, on page 105.

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

Step 2 Use the **Inventory** filter and search field to find the ASA device for which you want to create the NAT rule.

Step 3 In the **Management** area of the details panel, click **NAT** NAT.

Step 4 Click + > **Twice NAT**.

a. In section 1, select **Static.** Click **Continue**.

b. In section 2, select **Source Interface** = 'any' and **Destination Interface** = 'any'.Click **Continue**.

c. In section 3, select **Source Original Address** = 'any' and **Source Translated Address** = 'any'.

d. Select **Use Destination**.

1. **Destination Original Address** and **Source Translated Address**: Click **Choose** in the drop-down and select the network objects that match the configuration of the local IP address pools. In the below example, 'IPV4_Object' is the network object with the same configuration as the IPv4 address pool object used in the connection profile

and group policy settings of the ASA (BGL_ASA1_SH) device.

2. Select **Disable proxy ARP for incoming packets**.
3. Click **Save**.
4. Repeat the process (from step 4) to create equivalent rules for each of the other network objects equivalent to IP address pools.

Step 5 Deploy Configuration Changes from CDO to ASA.

Install the AnyConnect Client Software on ASA

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 ASA 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 ASA device, inform users to perform the following steps:

Note Android and iOS users should download AnyConnect from the appropriate App Store.

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.

Modify ASA Remote Access VPN Configuration

When ASA devices are onboarded to CDO, it discovers and displays the pre-existing remote access VPN configurations from onboarded ASA devices. For more information, see Manage and Deploy Pre-existing ASA Remote Access VPN Configuration.

You can modify these configurations and download the new configuration to the device.

Step 1 In the left pane, click **VPN** > **Remote Access VPN Configuration**.

Step 2 If you want to add or remove group policies to the VPN configuration, click the VPN configuration associated with the onboarded ASA device. In the Actions pane on the left, click **Group Policies**.

a) Click the blue + icon and configure the selections and click **Select**.

b) Click Save. You can also Create ASA Remote Access VPN Group Policies.

Step 3 Click the VPN configuration, and in the **Actions** pane, click **Edit**.

The wizard lists the ASA device associated with the configuration.

a) You can modify the following details in the same fashion as it was created:

- Change the name of the remote access VPN configuration.
- Click the three dots appearing in the row that shows the device details and click **Edit**.

For more information, see Create ASA Remote Access VPN Configuration, on page 290

Step 4 Click **OK**.

Step 5 Preview and Deploy Configuration Changes for All Devices, on page 233

Modify ASA Connection Profile

Step 1 In the left pane, click **VPN** > **Remote Access VPN Configuration**.

Step 2 Expand the VPN configuration associated with the onboarded ASA device, and select a connection profile.

Step 3 Under **Actions**, click **Edit**.

Step 4 Edit the values in the same fashion as it was created and click **Done**.

For more information, see Configure ASA Remote Access VPN Connection Profile, on page 294

Step 5 Preview and Deploy Configuration Changes for All Devices, on page 233

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.

CDO 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. CDO 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. CDO 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. CDO supports the FSP file format.
- **ISE Posture Profile** — Choose this option if you add a profile file for the AnyConnect ISE Posture module. CDO 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. CDO 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. CDO supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** — You must select this file type if you deploy the Umbrella Roaming Security module. CDO 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. CDO 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.

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 ASA Remote Access VPN Group Policies .

Note The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Verify ASA Remote Access VPN Configuration

After you configure the remote access VPN and deploy the configuration to the device, verify that you can make remote connections.

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 Install the AnyConnect Client Software on ASA . If you configured group URLs, also try those URLs.

Step 2 In the **Inventory** page, select the device (FTD or ASA) 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.

Step 6 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 ASA Remote Access VPN Configuration Details

Step 1 In the left pane, click **VPN** > **ASA/FDM 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 remote access 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. CDO 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 CDO.
- The live session screen shows the most used operating system and VPN connection profile in the CDO 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 315
- Monitor Historical AnyConnect Remote Access VPN Sessions, on page 316
- Search and Filter Remote Access VPN Sessions
- Customize the Remote Access VPN Monitoring View
- Export Remote Access VPN Sessions to a CSV File

- Disconnect all Active RA VPN Sessions of a User

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 CDO.
- Ensure that the connectivity status of the devices you want to monitor live data is "Online" on the **Inventory** page.

Step 1 In the left pane, click **VPN** > **Remote Access VPN Monitoring**.

Alternatively, you can click **View Active Remote Access VPN Sessions**on the CDO home page or navigate to **VPN** > **Remote Access VPN** and click the icon on the top-right corner of the screen.

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 CDO.

- **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 CDO 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 CDO 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 CDO.

Step 1 In the left pane, click **VPN** > **Remote Access VPN Monitoring**.

Alternatively, you can click **View Active Remote Access VPN Sessions** on the CDO home page or navigate to **VPN** > **Remote Access VPN** and click the icon in the top-right corner.

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 CDO. 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 CDO 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.

CDO remembers your selection the next time you sign in to CDO.

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, CDO creates a new .csv file, where the file created has a date and time in its name.

CDO 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.

Step 1 In the left pane, click **VPN** > **Remote Access VPN 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. CDO 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

CDO 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 **Dashboard**. The **RA VPN Sessions** provides the information in the following widgets:

- **VPN Tunnel Status**: Displays a pie chart representing the active and idle VPN tunnels, each in appropriate colors. This chart shows the top ten number of remote access VPN sessions by headends.
- **Statistics**: Shows the average session duration and data uploaded and downloaded.

By clicking **View All RA VPN Sessions**, you will be directed to the **Remote Access Monitoring** page, which lists all live and historical sessions.

Disconnect Remote Access VPN Sessions of an ASA User

You can terminate all active remote access VPN sessions of all users on the ASA device. You can perform this task in both live and historical modes.

CDO provides a VPN Sessions Manager user role to allow users to view and terminate VPN sessions. See User Roles in CDO for more information.

Step 1 In the left pane, click **VPN** > **Remote Access VPN Monitoring**.

Step 2 In the **View By Devices** area, click on the ASA device that you want to end all active sessions on that device.

Step 3 Click **Terminate All Sessions** appearing in the top-right corner.

Step 4 Click **Yes, Terminate All Sessions** to confirm your selection.

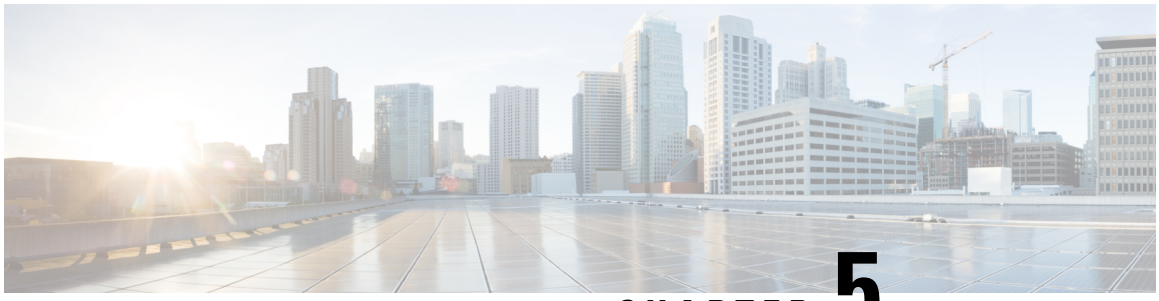
Disconnect all Active RA VPN Sessions of a User

CDO terminates all of the user's active RA VPN sessions on that ASA device when you disconnect a user. You can perform this task in both live and historical modes.

Step 1 In the left pane, click **VPN** > **Remote Access VPN Monitoring**.

Step 2 Search for a user whose sessions you want to disconnect. You can type the search criteria into the **Search** bar.

Step 3 Click on an active session, and in the **Actions** pane on the right, click the **Terminate all RA VPN sessions for this user** link.



CHAPTER 5

Monitoring and Reporting Change Logs, Workflows, and Jobs

CDO 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 CDO

A Change Log captures the configuration changes made in CDO, 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 CDO.
- 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

CDO 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 CDO's database and what you see in an exported change log. See Export the Change Log, on page 325 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 CDO:

- 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 CDO and are detected as conflicts, the **System User** is reported as the **Last User**.
- CDO closes a change log entry after a device's configuration on CDO is synced with the configuration on the device, or when a device is removed from CDO. Configurations are considered to be in sync after they read the configuration from the device to CDO or after deploying the configuration from CDO to the device.
- CDO 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 CDO is in sync with the configuration on the device (either by reading or deploying), or when CDO no longer manages the device.
- If a change is made to the device outside of CDO, 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 CDO, 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 CDO
- Deploying changes from CDO to a device
- Deleting a device from CDO
- Running a CLI command that updates the running configuration file

The following image is a Pending change log entry in an ASA. This is denoted by the open circle next to the timestamp.

Search and Filter Change Log Entries

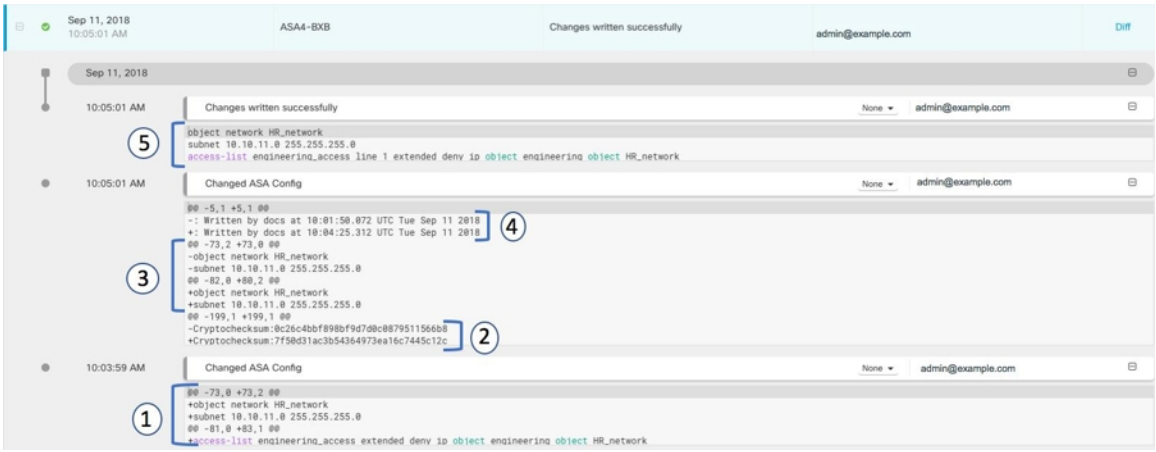
You can search and filter change log entries. Use the search field to find events. Use the filter ( ) to find the entries that meet the criteria you specify. You can also combine the two tasks by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

Change Log Entries after Deploying to an ASA

A checkmark on the header indicates that the change log is complete. The change log displays the most recent entries first followed by the older entries below in a chronological order. You can sort these entries.

Click the View Change Log Differences link in the change log entry row to view a side-by-side comparison of the changes in the context of the running configuration file.

The explanations for the different changes are shown below.

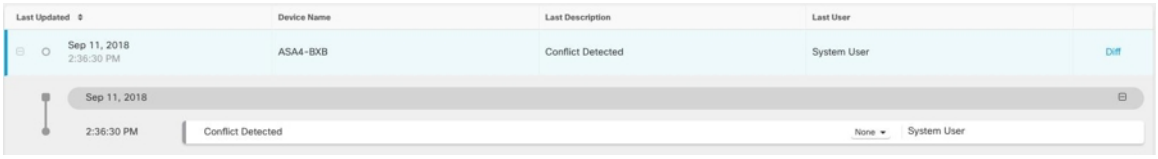


Number in illustration	Explanation
1	This is the change that admin@example.com made at 10:03:59 AM on September 11, 2018. **1.** The "HR_network" object was added. **2.** The initial network address (10.10.11.0) and subnet mask (255.255.255.0) were added to the I object. **3.** A rule was added to the "engineering_access" network policy denying addresses in the "engineer from reaching the "HR_network"
2	The checksum of the running configuration file was recalculated by the ASA and changed. The ol *removed* and the new value was *added*.
3	The ASA moves the object to a different location in the running configuration file than where Cis Orchestrator placed it. **Note** You don't always see this kind of an entry.

Number in illustration	Explanation
4	The record of the last time the running configuration file was updated. The old timestamp is removed new timestamp is added. This change was made by the ASA.
5	These are the commands sent by Cisco Defense Orchestrator to the ASA to make the configuration cl

Change Log Entries After Reading Changes from an ASA

When CDO detects a change on an ASA that it manages, it opens a change log entry and records the time when the configuration conflict was detected. You see this change log entry when CDO detects a conflict:



If you accept the changes, or review and accept the changes, that change is added to the change log entry and the entry is completed.

This entry shows the Conflict Detected change and the deletion of a rule that prevents addresses in the engineering network from reaching the HR_network. The change log entry also shows a change with the message *Successfully imported out-of-band changes.* If the admin chooses to reject the out-of-band change, the change log will display the message *Successfully rejected out-of-band changes on the device* along with what was rejected. Out-of-band changes refers to the changes made to the ASA device directly without using CDO.

Related Topics

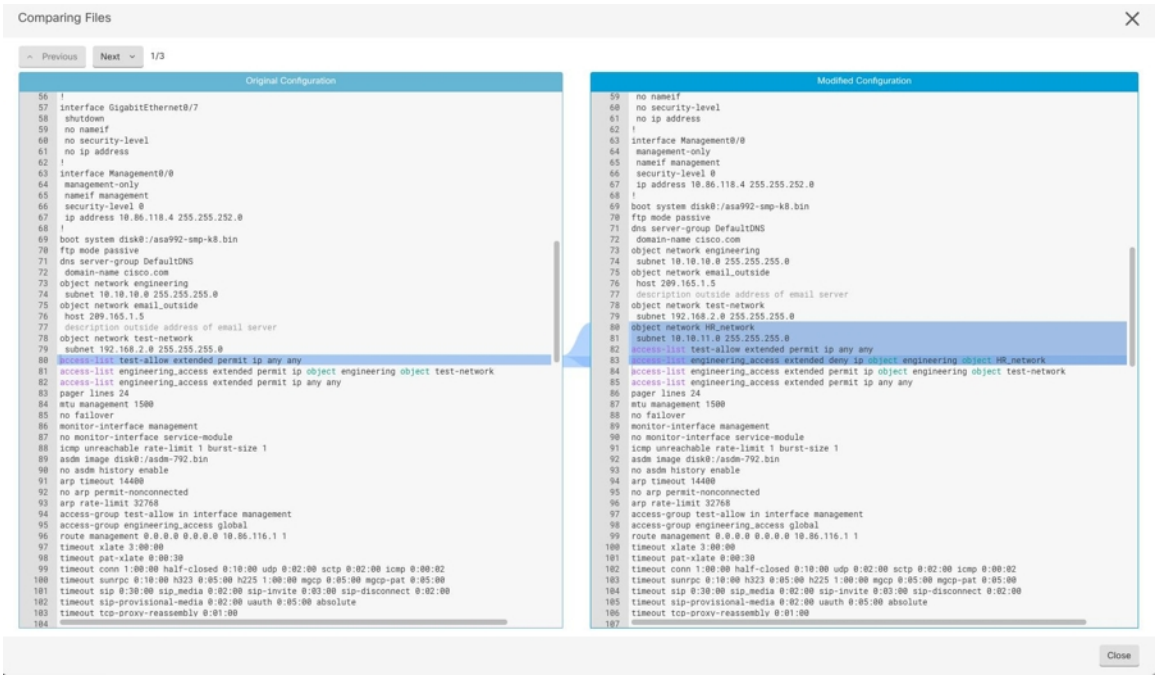
- Manage Change Logs in CDO, on page 321
- Change Log Entries after Deploying to an ASA, on page 323
- View Change Log Differences, on page 325
- About Device Configuration Changes

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 CDO, on page 321

Export the Change Log

You can export all or a subset of the CDO 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:

Step 1 In the left pane, click **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 CDO 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 CDO and Size of an Exported Change Log

The information that you export from CDO's Change Log page is different from the change log information that CDO stores in its database.

For every change log, CDO 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 CDO to display configuration differences side by side. In addition, CDO 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 CDO stores.

CDO 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 CDO and associate it with change log events. You can search for this change request by **Name** within the change log.

Note In CDO, **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.

Step 1 In the left pane, click **Settings** > **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

Step 1 In CDO, 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, CDO 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

Step 1 In the left pane, click **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

Step 1 In the left pane, click **Change Log**.

Step 2 In the change log search field, enter the name of a change request to find the associated change log events.

CDO highlights the change log events that are exact matches.

Search for a Change Request

Step 1 In CDO, 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

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

Step 1 In CDO, 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

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

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.

Step 1 In the left pane, click **Settings** > **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 327.
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 328 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 327. 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 327.
4. Clear the Change Request Toolbar, on page 328 to avoid automatic association of change log events with an existing change request.

Search for Change Log Events Associated with a Change Request

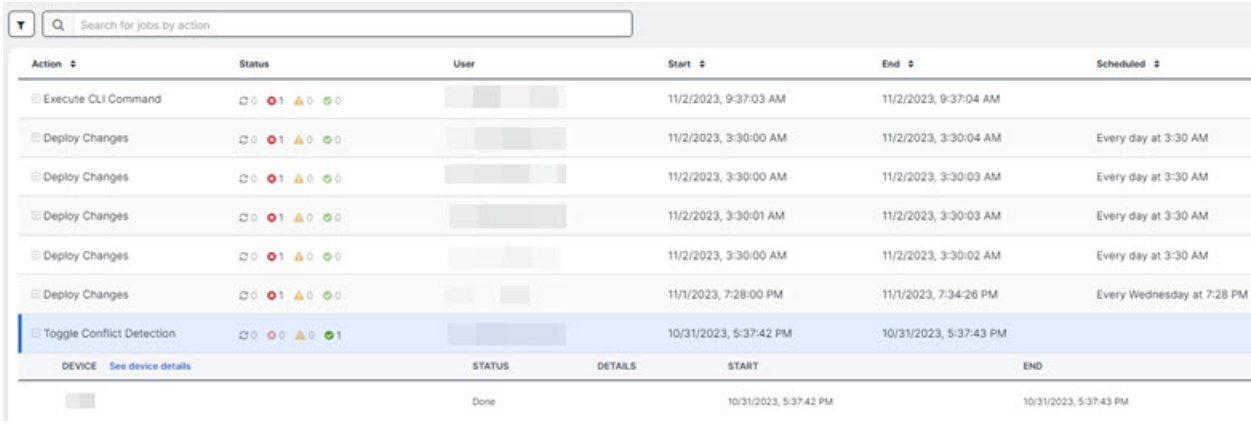
This use case describes a scenario where, you want to find out what change log events were recorded in the change log because of the work done to resolve a ticket maintained in an external system. Follow this procedure to search for change log events that are associated with a change request:

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. CDO highlights change log events that are exact matches.
   - Filter Change Requests, on page 328 to find the change log events.
3. View each change log to find the highlighted change log events showing the associated change request.

Monitor Jobs in CDO

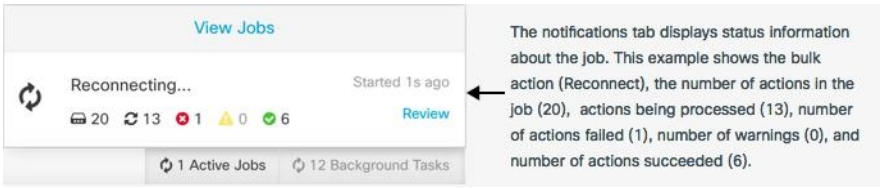
The **Jobs** page provides an overview of the progress of bulk operations, such as reconnecting multiple devices, reading configurations from multiple devices, or upgrading multiple devices simultaneously. The **Jobs** table uses color-coded rows along with the status of individual actions, indicating 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.



- From CDO, select **Jobs**. This table shows a complete list of the bulk actions performed in CDO.

Search Jobs in CDO

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 CDO will re-run the job only for the failed actions. To re-run a bulk action:

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:

Step 1 On the CDO navigation menu, click **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.

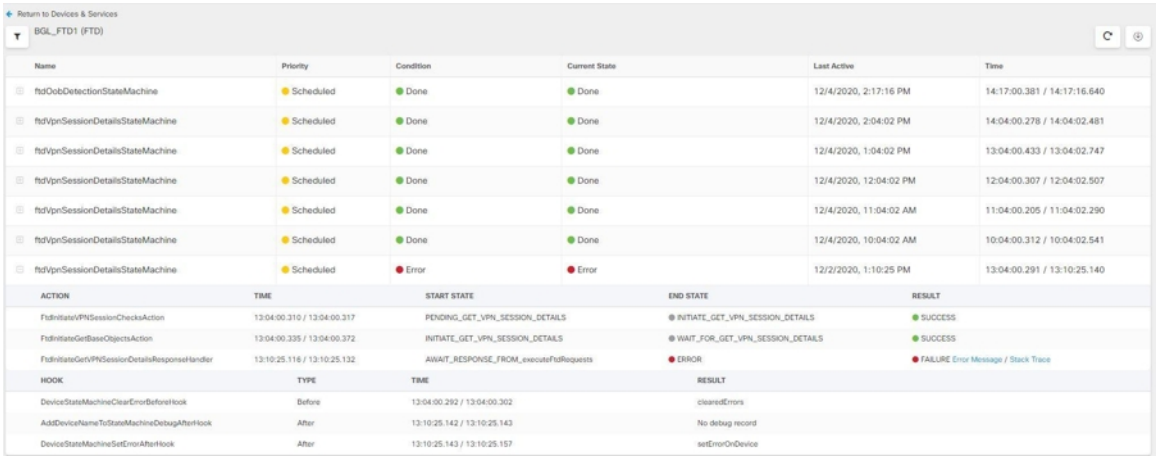
Monitor Workflows in CDO

The **Workflows** page allows you to monitor every process that CDO runs when communicating with devices, Secure Device Connector (SDC), or Secure Event Connector (SEC), and when applying ruleset changes to devices. CDO 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 CDO and not the device it is interacting with.

CDO 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, on the **Inventory** page, 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.

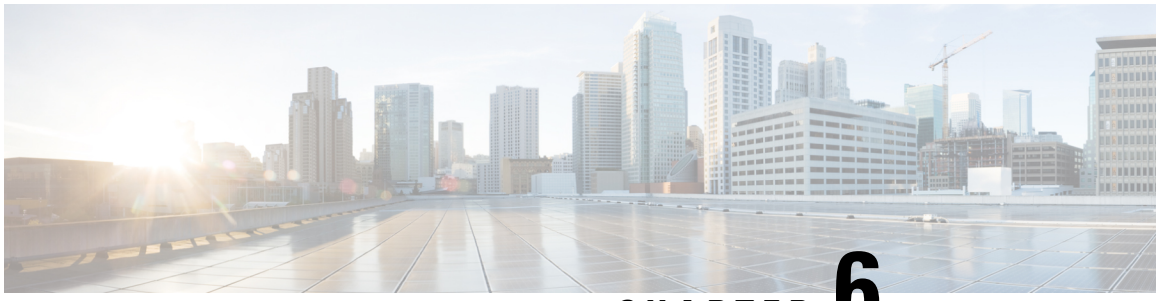


Export Device Workflows

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 6

Cisco Security Analytics and Logging

About Security Analytics and Logging (SaaS) in CDO

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 CDO. The events are stored in the Cisco cloud and viewable from the **Event Logging** page in CDO, 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 CDO 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 CDO

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 CDO supports. From the CDO 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 CDO 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

About Security Analytics and Logging (SAL SaaS) for the ASA

Security Analytics and Logging (SaaS) allows you to capture all syslog events and Netflow Secure Event Logging (NSEL) from your ASA and view them in one place in Cisco Defense Orchestrator.

The events are stored in the Cisco cloud and viewable from the Event Logging page in CDO 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 FTD 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 FTD events and your network traffic, and generates observations and alerts. You can cross-launch from CDO to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

How ASA Events are Displayed in the CDO Events Viewer

Syslog events and NSEL events are generated when logging is enabled on the ASA, and network traffic matches access control rule criteria. After the events are stored in the Cisco cloud, you can view them in CDO.

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. Do not forward the same events to all of your SECs. You will be duplicating the events sent to the Cisco cloud and needlessly inflate your daily ingest rate.

How Syslog and NSEL Events are Sent from an ASA to the Cisco Cloud by way of the Secure Event Connector

With the basic **Logging and Troubleshooting** license, this is how an ASA event reaches the Cisco cloud:

1. You onboard your ASA to CDO using username and password.
2. You configure the ASA to forward syslog and NSEL events to any one of your SECs as if they were syslog servers and enable logging on the device.
3. The SEC forwards the events to the Cisco cloud where the events are stored.
4. CDO displays events from the Cisco cloud in its Events Viewer 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 ASA syslog events stored in the Cisco cloud.
2. Generated observations and alerts are accessible from the Secure Cloud Analytics portal associated with your CDO portal.
3. From the CDO portal, you can cross-launch your Secure Cloud Analytics portal to review these observations and alerts.

Componets Used in the Solution

Secure Device Connector (SDC)-The SDC connects CDO to your ASAs. The login credentials for the ASA are stored on the SDC. See Secure Device Connector, on page 8 for more information.

Secure Event Connector (SEC)-The SEC is an application that receives events from your ASAs and forwards them to the Cisco cloud. Once in the Cisco cloud, you can view the events on CDO's Event Logging page or analyze them with Secure Cloud Analytics. Depending on your environment, the SEC is installed on a Secure Device Connector, if you have one; or on its own CDO Connector virtual machine that you maintain in your network. See Secure Event Connectors, on page 370 for more information.

Adaptive Security Appliance (ASA)-The ASA provides advanced stateful firewall and VPN concentrator functionality 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.

Secure Cloud Analytics applies dynamic entity modeling to ASA 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. You would make use of this service if you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license.

Licensing

To configure this solution you need the following accounts and licenses:

- **Cisco Defense Orchestrator**. You must have a CDO tenant.
- **Secure Device Connector**. There is no separate license for a Secure Device Connector.
- **Secure Event Connector**. There is no separate license for a Secure Event Connector.
- **Secure Logging Analytics (SaaS)**. See the Security Analytics and Logging License table.
- **Adaptive Security Appliance (ASA)**. Base license or higher.

Security Analytics and Logging Licensing

In order to implement Security Analytics and Logging (SaaS), you need to purchase one of these licenses:

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Logging and Troubleshooting	• View ASA events and event detail within CDO, both as a live feed and as a historical view	• 1 year • 3 years • 5 years	• CDO • An on-premises ASA deployment running software version 9.6 or greater. • Deployment of one or more SECs to pass ASA events to the Cisco 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 events. • Open alerts in Secure Cloud Analytics based on event data, cross-launching from the CDO event viewer.	• 1 year • 3 years • 5 years	• CDO • An on-premises ASA deployment running software version 9.6 or greater • Deployment of one or more SECs to pass ASA events to the Cisco cloud. • A newly provisioned or existing Cisco Secure Cloud Analytics portal.
Total Network Analytics and Monitoring	**Logging Analytics and Detection**, plus: • Apply dynamic entity modeling and behavioral analytics to ASA events, on-premises network traffic, and cloud-based network traffic • Open alerts in Cisco Secure Cloud Analytics based on the combination of ASA event data, on-premises network traffic flow data collected by Cisco Secure Cloud Analytics sensors, and cloud-based network traffic passed to Cisco Secure Cloud Analytics, cross-launching from the CDO event viewer.	• 1 year • 3 years • 5 years	• CDO • An on-premises ASA deployment running software version 9.6 or greater • Deployment of one or more SECs to pass events to the Cisco cloud. • Deployment of at least one Cisco Secure Cloud Analytics sensor version 4.1 or greater to pass network traffic flow data to the cloud OR integrating Cisco Secure Cloud Analytics with a cloud-based deployment, to pass network traffic flow data to Cisco Secure Cloud Analytics. • A newly provisioned or existing Cisco Secure Cloud Analytics portal.

Data Plans

You need to buy a data plan that reflects the number of events the Cisco cloud receives from your on-boarded ASAs on a daily basis. This is called your "daily ingest rate." You can use the Logging Volume Estimator Tool to estimate your daily ingest rate and as that rate changes you can update your data plan.

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 CDO and navigating **Monitoring** > **Event Logging** tab. 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.

Next Step

Go to Implementing Secure Logging Analytics (SaaS) for ASA Devices

Implementing Secure Logging Analytics (SaaS) for ASA Devices

Before you Begin

- Review About Security Analytics and Logging (SAL SaaS) for the ASAto 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 CDO Sales representative to create a CDO tenant.
- Review Secure Device Connector, on page 8. Connecting CDO to your ASA using an SDC is considered a "best practice" but it is not required.
- If you choose to deploy an SDC in your network, you can use one of these methods to install it:
  - Use Deploy a Secure Device Connector Using CDO's VM Image to install an SDC using CDO'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 have Installing Secure Event Connectors and you can send events from any ASA to any SEC onboarded to your tenant.
- You have Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication for users of your account.

Workflow to Implement Cisco Security Analytics and Logging (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud

1. Be sure to review "Before you Begin" above to make sure your environment is properly configured.
2. Onboard ASA Device to CDO, on page 127 using username and password.
3. Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface.
4. Configuring NSEL for ASA Devices by Using a CDO Macro.
5. Confirm events are visible in CDO. From the navigation bar, select **Monitoring > Event Logging**. Click the Live tab to view live events.
6. If you have a **Firewall Analytics and Monitoring** or **Total Network Analytics and Monitoring** license, continue with the next section, **Analyzing Events with Cisco Secure Cloud Analytics**.

Analyzing Events with Cisco Secure Cloud Analytics

If you have a **Firewall Analytics and Monitoring** 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 391.
2. Deploy one or more Secure Cloud Analytics sensors to your internal network if you purchased a **Total Network Analytics and Monitoring** license. See Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting, on page 392.
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 CDO, on page 393.
4. Cross-launch from CDO to Secure Cloud Analytics to monitor the Secure Cloud Analytics alerts generated from FTD events. See Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 393.

Reviewing Cisco Secure Cloud Analytics Alerts by Cross-launching from CDO

With a **Firewall Analytics and Monitoring** or **Total Network Analytics and Monitoring** license, you can cross-launch from CDO to Secure Cloud Analytics to review the alerts generated by FTD events.

Review these articles for more information:

- Sign in to CDO
- Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 393
- Cisco Secure Cloud Analytics and Dynamic Entity Modeling
- Working with Alerts Based on Firewall Events

Troubleshooting Secure Event Connector Issues

Use these troubleshooting topics to gather status and logging information about

- Troubleshooting SEC Onboarding Failures
- Event Logging Troubleshooting Log Files
- Use Health Check to Learn the State of your Secure Event Connector

Workflows

Troubleshooting Network Problems Using Security and Analytics Logging Events describes using the events generated from Cisco Security Analytics and Logging to determine why a user can't access a network resource.

See also Working with Alerts Based on Firewall Events.

Send ASA Syslog Events to the Cisco Cloud using a CDO Macro

You can configure all your ASAs to send events to the Cisco cloud by creating a CDO Macro that uses all the commands described in Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface and running that macro on all your ASA in the same batch.

CDO's Macro tool allows you to assemble a list of CLI commands, turn elements of the command syntax into parameters, and then save the list of commands so that it can be used more than once. Macros can also be run on more than one device at a time.

Using proven macros promotes configuration consistencies between devices and prevents syntax errors that can occur when using the command line interface.

Before you read further, review these topics so that you understand the mechanics of using macros. This article will only describe assembling the final macro.

- Command Line Interface Macros
- Create a CLI Macro from a New Command
- Run a CLI Macro
- Edit a CLI Macro
- Delete a CLI Macro

Creating an ASA Security Analytics and Logging (SaaS) Macro

There are two types of formatting you'll see in the following procedure, ASA CLI commands and macro formatting. The ASA CLI commands are written to follow ASA syntax conventions. The macro conventions are described in Create a CLI Macro from a New Command.

Before you begin, open Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface in a separate window and read it in parallel with this procedure so you can read the command descriptions as you create your macros.

Note If a logging config is already in place on the ASA, running the macro from CDO will *not* first clear out all of the existing logging config. Rather, the settings defined in the CDO macro will merge into whatever might already be in place.

Step 1 Open a plain text editor and create a list of commands you are going to turn into a macro, based on the instructions and options below. CDO will execute the commands in the order they are written in the macro. Some command will have values that you turn into {{parameters}} that you will fill in when it comes time to run the macro.

Step 2 **Configure the** ASA **to send messages to an SEC as if it were a syslog server.**

Use the **logging host** command to specify the SEC as the syslog server you send messages to. You can send events to any one of the SECs you have onboarded to your tenant.

The **logging host** command specifies a TCP or UDP port to send events to. SeeFinding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS) to determine what ports you should use.

logging host*interface_nameSEC_IP_address* { **tcp/port** | **udp/port** }

Turn this command into one of two different macros depending on what protocol you use to send syslog events to the SEC:

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

(Optional) If you use TCP, you can add this command to your list of commands in your macro. It does not need any parameters.

logging permit-hostdown

Step 3 **Specify which syslog messages should be sent to the syslog server.**

Use the **logging trap** command to specify which syslog messages should be sent to the syslog server:

logging trap { *severity_level* | *message_list* }

If you want to define the events sent to the SEC by severity level, turn the command into this macro:

logging trap {{severity_level}}

If you only want to send events to the SEC that are part of a message list, turn the command into this macro:

logging trap {{message_list_name}}

If you chose the **logging trap message_list** command in the previous step, you need to define the syslogs in your message list. Open Create a Custom Event List so you can read the command descriptions as you create the macro. Start with this command:

logging list*name* { **level***level* [**class***message_class*] | **message***start_id* [*-end_id*] }

And break it down into these variations:

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

In the last variation, the message parameter {{syslog_range_or_number}} could be entered as a single syslog ID, 106023, or a range, 302013-302018. Use one or more of the command variations in as many lines as you like to create your message list. Keep in mind that, in a single macro, all parameters with the same name will use the same value you enter. CDO will not run a macro with empty parameters.

Important The **logging list** command has to come before the **logging trap** command in your macro. You define the list first and then the **logging trap** command can use it. See the sample macro below.

Step 4 **(Optional) Add the syslog timestamp.** Add this command if you want to add the date and time to the message that the syslog message originated on the ASA. The timestamp value is displayed in the **SyslogTimestamp** field. Add this command to your list of commands, it will not need any parameters:

logging timestamp

Note Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. Following is a sample output with RFC 5424 format:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port
```

.

Step 5 **(Optional) Include a device ID in non-EMBLEM format syslog messages.** Open Include the Device ID in Non-EMBLEM Format Syslog Messages so you can read the command descriptions as you create the macro. This is the CLI command you will base your macro on:

logging device-id { **cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text* }

And break it down into these variations:

logging device-id cluster-id

logging device-id context-name

logging device-id hostname

logging device-id ipaddress {{interface_name}} **system**

logging device-id string {{text_16_char_or_less}}

Step 6 **Enable logging**. Add this command to your macro as it is. It does not have any parameters:

logging enable

Step 7 **Do not add write memory** to the last line of the macro. Add the **show running-config logging** command instead to review the results of the logging commands you entered before committing them to the ASA's startup config.

show running-config logging

Step 8 After you are confident your configuration changes were made, you can create a separate macro for the **write memory** command or use CDO's Bulk CLI Interface function to issue the command to all the devices you configured using your macro.

write memory

Step 9 **(Optional) Enable logging on access control rule "permit" events.** This step in the described in the Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface procedure but it is not included in this macro. It is performed in the CDO GUI instead.

Step 10 Save the macro.

Example

Here is a sample of a list of commands combined into a single macro:

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

Note There are several logging list commands to add different specific syslog IDs or ranges. The {{syslog_range_or_number_X}} parameter requires a number or some other differentiator, otherwise their values will all be the same when the macro is filled in. Also keep in mind that CDO will not run a macro if not all the parameters are given a value, so only include the commands in the macro you want to execute. We do want all the syslog IDs contained in the same list so event_list_name stays the same for in each line.

What to do next

Run the Macro

After you have created and saved the ASA Security Analytics and Logging Macro, run the macro to send ASA syslog events to the Cisco cloud.

Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface

This procedure explains how to forward ASA syslog events to a Secure Event Connector (SEC) and then enable logging. These procedures explain only what is needed to complete that workflow. For a broader discussion of all the ways you can configure logging on the ASA, see the Monitoring chapter of either ASDM1: Cisco ASA Series General Operations ASDM Configuration Guide or CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide.

Limitations on Supported ASA Commands

CDO does not yet support these syslog commands or message formats:

- EMBLEM format for syslogs
- Secure Syslogs

CDO Command Line Interface for ASA

For all the tasks in this procedure, you will be working on the CDO's command line interface for ASA. To open the command line interface page:

Step 1 From the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the ASA for which you want to enable logging.

Step 4 In the Device Actions pane on the right, click **>_ Command Line Interface**.

Step 5 Click the **Command Line Interface** tab. You are now ready to enter the commands described below at the prompt.

After entering every command, you will click **Send**. Because CDO's CLI Interface is a direct connection to the ASA, the command is written to the device's running configuration immediately. For changes to be written to the ASA's startup configuration, you need to issue the `write memory` command in addition.

Forward ASA Syslog Events to the Secure Event Connector

To forward ASA syslog events to one of the Secure Event Connectors (SECs) you have onboarded and then enable logging, you need complete these tasks in the procedure that follows.

Step 1 Configure the ASA to send messages to the SEC as if it were a syslog server.

Step 2 Decide what severity level of all logs, or what list of syslog events, you want to send to the SEC.

Step 3 Enable logging.

Step 4 Save the changes to the ASA's startup config.

Send ASA Syslog Events to the Cisco Cloud Using CLI

Step 1 **Configure the** ASA **to send messages to the SEC as if it were a syslog server**

When sending syslog events from the ASA to the Cisco cloud, you forward them to the SEC as if it were an external syslog server, and it forwards the messages to the Cisco cloud.

To send syslog messages to the SEC, perform the following steps:

a. Configure the ASA to send messages, using TCP or UDP, to the SEC as if it were a syslog server. The SEC can use an IPv4 or IPv6 addresss. You will be sending events to either a TCP or UDP port. See Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS) to determine what ports you should use.

Here is an example of the **logging host** command syntax:

logging host *interface_name SEC_IP_address* [[**tcp/port**] | [**udp/port**]]

Examples:

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- The **interface_name** argument specifies the ASA interface from which messages are sent to the syslog server. It is a "best practice" to send the syslog messages to the SDC over the same ASA interface already in use for communication with the SDC.
- The **SEC_IP_address** argument should contain the IP address of the VM on which the SEC is installed.
- The **tcp/port** or **udp/port** keyword-argument pair specifies that syslog messages should be sent using either TCP protocol and relevant port, or the UDP protocol and relevant port. You can configure the ASA to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol.

  If you specify TCP, the ASA will discover syslog server failures and as a security protection, new connections through the ASA are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see step b. If you specify UDP, the ASA continues to allow new connections whether or not the syslog server is operational. Valid port values

  Note If you want to send ASA messages to two separate syslog servers, you can run a second logging host command with the appropriate interface, IP address, protocol and port of the other syslog server.

b. (Optional) If you send events to the SEC over TCP, and if either the SEC is down or the log queue on the ASA is full, then new connections are blocked. New connections are allowed again after the syslog server is back up and the log queue is no longer full. To allow new connections regardless of connectivity to a TCP syslog server, disable the feature to block new connections when a TCP-connected syslog server is down using this command:

logging permit-hostdown

Example:

```
 > logging permit-hostdown
```

Step 2 **Specify which syslog messages should be sent to the syslog server with the following command:**

logging trap { severity_level | message_list }

Examples:

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

You can specify the severity level number (1 through 7) or name. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

The message_list argument is replaced with the name of a custom event list, if you have created one. When specifying a custom event list, you only send the syslog messages that are in that list to the Secure Event Connector. In the example above, asa_syslogs_to_cloud is the name of the event list.

Using a message_list could save you money by tightly defining which syslog messages are sent to the Cisco cloud.

See Create a Custom Event List to create a message_list. See Data Storage Plans for more information about data ingest and storage costs.

Step 3 **(Optional) Add the syslog timestamp**

Add the date and time that the syslog message originated on the ASA to the message using the logging timestamp command. The timestamp value is displayed in the **SyslogTimestamp** field.

Example:

```
> logging timestamp
```

Note Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. Following is a sample output with RFC 5424 format:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port.
```

Step 4 (Optional) Include a device ID in non-EMBLEM format syslog messages

A device ID is an identifier you can insert in a syslog message that will help you easily distinguish all syslog messages sent from a particular ASA. See Include the Device ID in Non-EMBLEM Format Syslog Messages for instructions.

Step 5 (Optional) Enable logging on access control rule "permit" events

When an access control rule denies access to a resource, the event is automatically logged. If you also want to log events generated when an access control rule allows access to a resource, you need to turn on logging for the access control rule and configure a severity type. See About System Log Activity for instructions on how to turn on logging for an individual network access control rule.

Note Enabling logging on access control rule "permit" events will use-up more of your purchased data plan as it is based on your daily ingest rate of events.

Step 6 Enable logging

At the command prompt, type logging enable. On the ASA, logging is enabled for the entire device, not for individual rules.

Example:

```
 > logging enable
```

Note At this time, CDO does not support enabling secure logging.

Step 7 Save your Changes to the Startup Config

At the command prompt, type write memory. On the ASA, logging is enabled for the entire device, not for individual rules.

Example:

```
> write memory
```

Related Infromation:

- Install a Secure Event Connector on an SDC Virtual Machine, on page 371
- Installing an SEC Using a CDO Image

Create a Custom Event List

Create a custom event list when you are sending ASA syslog events to the Cisco Cloud using one of these methods:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Send ASA Syslog Events to the Cisco Cloud using a CDO Macro

You can create an event list, also referred to as a message_list, based on the following three criteria:

- Event Class
- Severity
- Message ID

To create a custom event list to send to a specific logging destination (for example, a syslog server or a Secure Event Connector), perform the following steps:

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate tab and select the ASA whose syslog messages you want to include in a custom event list.

Step 4 In the **Device Actions** pane, click **>_ Command Line Interface.**

Step 5 Use this command syntax to issue the **logging list** command to the ASA:

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id* [*-end_id*] }

The *name* argument specifies the name of the list. The **level** *level* keyword and argument pair specify the severity level. The **class** *message_class* keyword-argument pair specify a particular message class. The **message** *start_id* [*-end_id*] keyword-argument pair specify an individual syslog message number or a range of numbers.

Note Do not use the names of severity levels as the name of a syslog message list. Prohibited names include emergencies, alert, critical, error, warning, notification, informational, and debugging. Similarly, do not use the first three characters of these words at the beginning of an event list name. For example, do not use an event list name that starts with the characters "err."

- **Add syslog messages to the event list based on severity**. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

  Example:

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- **Add syslog messages based on other criteria to the event list**:

  Enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion that you want to add to the list. For example, you can specify criteria for syslog messages to be included in the list as the following:

  - Syslog message IDs that fall into the range of 302013-302018.
  - All syslog messages with the critical severity level or higher (emergency, alert, or critical).
  - All HA class syslog messages with the warning severity level or higher (emergency, alert, critical, error, or warning).

Example:

```
> logging list asa_syslogs_to_cloud message 302013-302018
> logging list asa_syslogs_to_cloud level critical
> logging list asa_syslogs_to_cloud level warning class ha
```

Note A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

Step 6 **Save your Changes to the Startup Config**

At the command prompt, type **write memory**.

Example:

```
> write memory
```

Include the Device ID in Non-EMBLEM Format Syslog Messages

You can configure the ASA to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages. This procedure is referred to by these procedures:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Send ASA Syslog Events to the Cisco Cloud using a CDO Macro

This device identifier will be reflected in the SensorID field of a syslog event displayed on the Event Logging page.

Step 1 Select the ASA whose syslog messages you want to assign a device-id to.

Step 2 In the Device Actions pane, click **>_ Command Line Interface.**

Step 3 Use this command syntax to issue the **logging device-id** commands to the device.

logging device-id { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **string***text* }

Example:

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

Note In an ASA cluster, always use the primary unit IP address for the selected interface.

The **cluster-id** keyword specifies the unique name in the boot configuration of an individual ASA unit in the cluster as the device ID.

The **hostname** keyword specifies that the hostname of the ASA should be used as the device ID.

The **ipaddress** *interface_name* keyword-argument pair specifies that the interface IP address specified as *interface_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified ASA interface IP address, regardless of the interface from which the syslog message is sent. In the cluster environment, the **system** keyword dictates that the device ID becomes the system IP address on the interface. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device.

The **string** *text* keyword-argument pair specifies that the text string should be used as the device ID. The string can include as many as 16 characters.

You cannot use blank spaces or any of the following characters:

- & (ampersand)
- ‘ (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)

Step 4 **Save your Changes to the Startup Config**

At the command prompt, type **write memory**.

Example:

```
> write memory
```

NetFlow Secure Event Logging (NSEL) for ASA Devices

Basic syslog messages from the ASA lack much of the data that Secure Cloud Analytics needs to determine if events reported by the ASA indicate a threat. Netflow Secure Event Logging (NSEL) provides the Secure Cloud Analytics with that data.

"A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flows are highly granular; for example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, etc."[1]

The Cisco ASA supports NetFlow Version 9 services. The ASA implementation of NSEL provides a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes.

This documentation describes a straight forward approach to configuring NetFlow for your ASAs using a CDO macro. The Cisco ASA NetFlow Implementation Guide provides an extremely detailed discussion of configuring NetFlow on the ASA and you may find it a valuable resource to accompany this content.

What to do Next

Go to Configuring NSEL for ASA Devices by Using a CDO Macro.

Related Articles

- Configuring NSEL for ASA Devices by Using a CDO Macro
- Delete NetFlow Secure Event Logging (NSEL) Configuration from an ASA
- Determine the Name of an ASA Global Policy

1. ("Cisco Systems NetFlow Services Export Version 9." Internet Engineering Task Force, Network Working Group, Request for Comments: 3954, October 2004, B. Claise, Ed. https://www.ietf.org/rfc/rfc3954.txt)

Configuring NSEL for ASA Devices by Using a CDO Macro

ASAs report detailed connection event data using Netflow Secure Event Logging (NSEL). You can apply Secure Cloud Analytics to this connection event data, which includes bidirectional flow statistics. This procedure describes how to configure NSEL on an ASA device and send those NSEL events to a flow collector. In this case, the flow collector is a Secure Event Connector (SEC).

This procedure refers to this macro, **Configure NSEL**:

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

Here is an example of the Configure NSEL macro with all the default values filled in, a generic name for the class-map, and the class map added to the global_policy, When you are done with these procedures, your macro will resemble this:

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

Before you Begin

Gather the following information:

- Read these topics if you have never worked with a CDO Macro before:
  - Command Line Interface Macros, on page 217
    - Edit a CLI Macro, on page 221

- Run a CLI Macro, on page 220

- IPv4 address of the SEC that will receive data from the ASA
- Interface on the asa that will send data to the SEC
- UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS), on page 451.
- Determine the Name of an ASA Global Policy, on page 364

Workflow

Follow this workflow to configure NSEL for ASA devices by using a CDO macro. You need to follow each step:

1. Open the Configuring NSEL Macro , on page 358.
2. Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC, on page 359.
3. Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC, on page 360.
4. Define a Policy-Map for NSEL Events, on page 360.
5. Disable Redundant Syslog Messages, on page 361.
6. Review and Send the Macro, on page 362.

What to do next

Begin the workflow above by going to Open the Configuring NSEL Macro , on page 358.

Open the Configuring NSEL Macro

Before you begin

This is first part in a longer workflow, see Configuring NSEL for ASA Devices by Using a CDO Macro, on page 357 before getting started.

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the appropriate device type tab and select the ASA(s) on which you want to configure NetFlow Secure Event Logging (NSEL).

Step 3 In the **Device Actions** pane, click **Command Line Interface**.

Step 4 Click the Macro star  Macros to show the list of available macros.

Step 5 From the list of macros, select **Configuring NSEL**.

Step 6 Under the Macro box, click **View Parameters**.

What to do next

Continue to Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC, on page 359.

Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC

NSEL messages can be sent to any one of the SECs you have onboarded to your tenant. These instructions refer to this section of the macro:

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA Devices by Using a CDO Macro, on page 357 before getting started.

Step 1 The **flow-export destination** command defines the collector to which the NetFlow packets are sent. In this case, you are sending them to an SEC. Fill in the fields for these parameters:

- **{{interface}}**-Enter the name of the interface on the ASA from which the NetFlow events are sent.
- **{{SEC_IPv4_address}}**-Enter the IPv4 address of the SEC. The SEC functions as the flow collector.
- **{{SEC_NetFlow_port}}**-Enter the UDP port number on the SEC to which NetFlow packets are sent.

Step 2 The **flow-export template timeout-rate** command specifies the interval at which template records are sent to all configured output destinations.

- **{{timeout_rate_in_mins}}**-Enter the number of minutes before templates are resent. **We recommend using a value of 60 minutes**. The SEC does not process the templates. A large number reduces traffic to the SEC.

Step 3 The **flow-export delay flow-create** command delays the sending of flow-create events by the specified number of seconds. This value matches the recommended Active Timeout value and reduces the number of flow events exported from the ASA. At that rate, expect NSEL events to first appear in CDO at the close of a connection or within 55 seconds of the creation of the connection, whichever happens earlier. If this command is not configured, there is no delay, and the flow-create event is exported as soon as the flow is created.

- **{{delay_flow_create_rate_in_secs}}**-Enter the number of seconds delay between sending flow-create events. **We recommend using a value of 55 seconds**.

Step 4 The **flow-export active refresh-interval** command defines the frequency that status updates for long-lived flows will be sent from ASA. Valid values are from 1-60 minutes. In the Flow Update Interval field, configuring the **flow-export active refresh-interval** to be at least 5 seconds more than the **flow-export delay flow-create** interval prevents flow-update events from appearing before flow-creation events.

- **{{refresh_interval_in_mins}}-We recommend using a value of 1 minute**. Valid values are from 1-60 minutes.

What to do next

Continue to Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC, on page 360.

Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC

The following commands in the macro group all NSEL events in a class and then export that class to the Secure Event Connector (SEC). These instructions refer to this section of the macro:

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA Devices by Using a CDO Macro, on page 357 before getting started.

Step 1 The **class-map** command names the class map that identifies NSEL traffic that will be exported to the SEC.

- **{{flow-export-class-name}}**-Enter a name for your class map. The name may be up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot re-use a name already used by another type of class map.

Step 2 Identify the traffic that is going to be associated with (matched with) your class-map. Choose one of these options for the value of **{{add_this_traffic_to_class_map}}:**

- Enter **any** in the **{{add_this_traffic_to_class_map}}** field. This monitors all traffic types for NSEL traffic. **We recommend using the value "any".**
- Enter **access-list** ***name-of-access-list*** in the **{{add_this_traffic_to_class_map}}** field. This associates all the traffic associated with an access-list that you have created. See Configure Flow-Export Actions Through Modular Policy Framework in the Cisco ASA NetFlow Implementation Guide for more information.

What to do next

Continue to, Define a Policy-Map for NSEL Events, on page 360.

Define a Policy-Map for NSEL Events

The task assigns NetFlow export actions to the class you created in the previous task, and the class to a new policy map. These instructions refer to this section of the macro:

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA Devices by Using a CDO Macro, on page 357 before getting started.

Step 1 The **policy-map** command creates a policy-map. In the next task, you associate this policy map with the global policy.

- **{{global_policy_map_name}}**-Enter a name for the policy map. **We recommend using the name of the firewall's existing global policy if there is one**. The default name for the global policy is **global_policy**. See Determine the Name of an ASA Global Policy. If you create a new policy map and apply it globally according to Configure Flow-Export Actions Through Modular Policy Framework in Cisco ASA NetFlow Implementation Guide, the remaining inspection policies are deactivated.

Step 2 The **class** command inherits the name of the class-map you created in Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC, on page 360.

Step 3 The **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} command defines which event types should be sent to flow collector, (in this case the SEC).

- **{{event-type}}**-The event_type keyword is the name of the supported event being filtered. **We recommend using the value "all"**.
- **{{SEC_IPv4_address}}**-This is the IPv4 address of the SEC. Its value is inherited from the value you entered in Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC, on page 359.

What to do next

Continue to, Disable Redundant Syslog Messages, on page 361.

Disable Redundant Syslog Messages

These instructions refer to this section of the macro. You do not need to modify the command.

logging flow-export-syslogs disable

Enabling NetFlow to export flow information makes the syslog messages in the following table redundant. In the interest of performance, we recommend that you disable redundant syslog messages, because the same information is exported through NetFlow.

Note When NSEL and syslog messages are both enabled, there is no guarantee of chronological ordering between the two logging types.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
106100	Generated whenever an access control rule (ACL) is encountered.	1-Flow was created (if the ACL allowed the flow). 3-Flow was denied (if the ACL denied the flow).	0-If the ACL allowed the flow. 1001-Flow was denied by the ingress ACL. 1002-Flow was denied by the egress ACL.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
106015	A TCP flow was denied because the first packet was not a SYN packet.	3-Flow was denied.	1004-Flow was denied because the first packet was not a TCP SYN packet.
106023	When a flow was denied by an ACL attached to an interface through the **access-group** command.	3-Flow was denied.	1001-Flow was denied by the ingress ACL. 1002-Flow was denied by the egress ACL.
302013, 302015, 302017, 302020	TCP, UDP, GRE, and ICMP connection creation.	1-Flow was created.	0-Ignore.
302014, 302016, 302018, 302021	TCP, UDP, GRE, and ICMP connection teardown.	2-Flow was deleted.	0-Ignore. > 2000-Flow was torn down.
313001	An ICMP packet to the device was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.
313008	An ICMP v6 packet to the device was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.
710003	An attempt to connect to the device interface was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.

If you do not want to disable redundant syslog messages, you can edit this macro and delete only this line from it:

logging flow-export-syslogs disable

You can later enable or disable individual syslog messages by following the procedure in the Disabling and Reenabling NetFlow-related Syslog Messages.

Review and Send the Macro

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA Devices by Using a CDO Macro, on page 357, before getting started.

Step 1 After filling in the fields of the macro, click **Review** to review the commands before they are sent to the ASA.

Step 2 If you are satisfied with your responses to the commands, click **Send**.

Step 3 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 changes in the running-configuration, to the device's startup configuration.
- Clicking **Dismiss** dismisses the message.

You have finished the workflow descried in Configuring NSEL for ASA Devices by Using a CDO Macro, on page 357.

Delete NetFlow Secure Event Logging (NSEL) Configuration from an ASA

This procedure explains how to DELETE the NetFlow Secure Event Logging (NSEL) Configuration on an ASA, which specifies the Secure Event Connector (SEC) as the NSEL flow collector. This procedure reverses the macro described in Configuring NSEL for ASA Devices by Using a CDO Macro.

This procedure refers to this macro, **DELETE NSEL**:

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

Open the DELETE-NSEL Macro

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the appropriate device type tab and select the ASA(s) on which you want to delete the configuration of NetFlow Secure Event Logging (NSEL).

Step 3 In the **Device Actions** pane, click **Command Line Interface**.

Step 4 Click the Macros star 

to show the list of available macros.

Step 5 In the list of macros, select **DELETE-NSEL**.

Step 6 Under the Macro box, click **View Parameters**.

Enter the Values in the Macro to Complete the No Commands

The ASA CLI uses the "no" form of a command to delete it. Fill in the fields in the macro to complete the "no" form of the command:

Step 1 policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}**-Enter the value of the policy-map name.

Step 2 no class {{flow_export_class_name}}

- **{{flow_export_class_name}}**-Enter the value of the class-map name.

Step 3 no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}**-The value of the class-map name is inherited from the step above.

Step 4 no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}**-Enter the name of the interface on the ASA from which the NetFlow events were sent.
- **{{IPv4_address}}**-Enter the IPv4 address of the SEC. The SEC functions as the flow collector.
- **{{NetFlow_port}}**-Enter the UDP port number on the SEC to which NetFlow packets were sent.

Step 5 no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}**-Enter the flow-export template timeout-rate.

Step 6 no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}**-Enter the flow-export delay flow-create rate.

Step 7 no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}**-Enter the flow-export active refresh-interval interval.

Determine the Name of an ASA Global Policy

To determine the name of the ASA's global policy, follow this procedure:

Step 1 From the **Inventory** page, select the device for which you want to find the name of the global policy.

Step 2 In the Device Actions pane, select **>_Command Reference**.

Step 3 In the Command Line Interface window, at the prompt, type:

show running-config service-policy

In the output of the example below, global_policy is the name of the global policy.

Example:

> **show running-config service-policy**

service-policy global_policy global

Troubleshooting NSEL Data Flows

Once you have Configuring NSEL for ASA Devices by Using a CDO Macro , 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

Verify that NSEL Events are Being Sent to the SEC

Use one of two commands to verify that NSEL packets are being sent to the SEC:

- flow-export counters
- capture

Use the "flow-export counters" Command to Check for flow-export Packets Being Sent and for NSEL errors

- Make sure you have configured your ASA to send NSEL events to the SEC. See Configuring NSEL for ASA Devices by Using a CDO Macro.
- The SEC IP address is the flow collector address for NSEL events. If you have onboarded more than one SEC to your tenant, be sure you are using the correct IP address.
- Find the UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS).
- Our recommended interface on the ASA from which to send NSEL events is the management interface; your interface may be different.

Use the Bulk Command Line Interface in CDO to send these commands to the ASAs that you have configured for NSEL.

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device tab and select the ASA you configured to send NSEL events to the SEC.

Step 4 In the **Device Actions** pane on the right, click **Command Line Interface**.

Step 5 Reset the flow export counters by running the `clear flow-export counters` command. This resets the clear export flow counters to zero so that you can easily tell if new events are coming in.

example:

```
> clear flow-export counters

Done!
```

Step 6 Run the show flow-export counters command to see the destination of the NSEL packets, how many packets were sent and any errors:

example:

```
>show flow-export counters

destination: management 209.165.200.225 10425

Statistics:

packets sent 25000

Errors:

block allocation errors 0

invalid interface 0

template send failure 0

no route to collector 0

source port allocation 0
```

In the output above, the destination line shows the interface on the ASA from which NSEL events are sent, the IP address of the SEC, port 10425 of the SEC. It also shows packets sent of 25000.

If there are no errors and packets are being sent, skip to Verify that NetFlow Packets are Being Received by the Cisco Cloud below.

Error descriptions:

- **block allocation errors**-If you receive a block allocation error, the ASA did not allocate memory to the flow-exporter.
  - Recovery action: Call Cisco Technical Assistance Center (TAC).
- **invalid interface**-Indicates that you are trying to send NSEL events to the SEC but the interface you've defined for flow export isn't configured to do so.
  - Recovery action: Review the interface you chose when configuring NSEL. We recommend using the management interface, your interface may be different.
- **template send failure**-The template you had to define NSEL was not parsed correctly.
  - Recovery action: Contact CDO Support.
- **no route to collector**-Indicates there is no network route from the ASA to the SEC.
  - Recovery actions:

- Make sure that the IP address you used for the SEC when you configured NSEL is correct.
- Make sure the SEC's status is Active and it has sent a recent heartbeat. See SDC is Unreachable, on page 478.
- Make sure the Secure Device Connector's status is Active and it has sent a recent heartbeat.

- **source port allocation**-May indicate that there is a bad port on your ASA.

Use the "capture" Command to Capture NSEL Packets Sent from the ASA to the SEC

- Make sure you have configured your ASA to send NSEL events to the SEC. See Configuring NSEL for ASA Devices by Using a CDO Macro.
- The SEC IP address is the flow collector address for NSEL events. If you have onboarded more than one SEC to your tenant be sure you are using the correct IP address.
- Find the UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS)
- Our recommended interface on the ASA from which to send NSEL events is the management interface; your interface may be different.

Use the CDO Command Line Interface in CDO to send these commands to the ASAs that you have configured for NSEL.

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the ASA you configured to send NSEL events to the SEC.

Step 4 In the **Device Actions** pane on the right, click **Command Line Interface**.

Step 5 In the command window, run this **capture** command:

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

Where

- *capture_name* is the name of the packet capture.
- *interface_name* is the name of the interface from which NSEL packets leave the ASA.
- *IP_of_SEC* is the IP address of the SEC VM.
- *NetFlow_port* is the port to which NSEL events are sent.

This starts the packet capture.

Step 6 Run the **show capture** command to view the captured packets:

> **show capture***capture_name*

Where *capture_name* is the name of the packet capture you defined in the previous step.

Here is an example of the output showing the time of the capture, the IP address from which the packet was sent, the IP address, and the port the packet was sent to. In this example, 192.168.25.4 is the IP address of the SEC and port 10425 is the port on the SEC that receives NSEL events.

```
6 packets captured
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

Step 7 Run the **capture stop** command to manually stop the packet capture:
> capture *capture_name***stop**

Where *capture_name* is the name of the packet capture you defined in the previous step.

Verify that NetFlow Packets are Being Received by the Cisco Cloud

Before you Begin

Verify that NSEL events are being sent from the ASA.

Check for Live NSEL Events

Check for both live and historical events.

This procedure will filter for NSEL events that the Cisco Cloud has received within the last hour.

Step 1 In the left pane, choose **Analytics** > **Event Logging**.
Step 2 Click the **Live** tab.
Step 3 Pin-open the event filter.
Step 4 In the ASA Events section, make sure NetFlow is checked.
Step 5 In the Sensor ID field, enter the IP address of the ASA you configured to send NSEL events.
Step 6 At the bottom of the filter, make sure that "Include NetFlow Events" is checked.

Check for Historical NSEL Events

This procedure will filter for NSEL events that the Cisco Cloud has received within the time-frame you specify.

Step 1 In the left pane, choose **Analytics** > **Event Logging**.
Step 2 Click the **Historical** tab.
Step 3 Pin-open the event filter.
Step 4 In the ASA Events section, make sure NetFlow is checked.
Step 5 Set the Start time far enough back in time to check if CDO ever did receive NSEL events.

Step 6 In the Sensor ID field, enter the IP address of the ASA you configured to send NSEL events.

Step 7 At the bottom of the filter, make sure that "Include NetFlow Events" is checked.

Parsed ASA Syslog Events

Parsed syslog events contain more event attributes than other syslog events and let you search on any specific parsed field. The SEC forwards all ASA events you specify to the Cisco cloud but only the syslog messages in the table below are parsed. All parsed Syslogs events are shown with their EvenTypes italicised to help you identify.

For detailed explanations of syslogs see, Cisco ASA Series Syslog Messages.

Syslog ID	Syslog Category	Purpose of syslog messge
106015	Firewall	Represents out of state TCP Deny
106023	Firewall	A real IP packet was denied by the ACL. This message appears even if you do not have the **log** option enabled for an ACL.
106100	Access Lists/User Session	Packet was permitted or denied by an ACL.
113019	User Authentication	Critical AnyConnect
302013, 302015, 302017, 302020	User Session	Connection start and end syslogs for TCP, UDP, GRE, and ICMP connection creation.
302014, 302016, 302018, 302021	User Session	Connection start and end syslogs for TCP, UDP, GRE, and ICMP connection creation.
302020 - 302021	User Session	ICMP session establishment and teardown.
305006	User Session/NAT and PAT	NAT connection failure
305011-305014	User Session/NAT and PAT	NAT Build/Teardown related
313001, 313008	IP Stack	Represents denied connections to the box.
414004	System	Critical AnyConnect
609001 - 609002	Firewall	A network state container was reserved/removed for host **ip-address** connected to a zone.
710002,710004 710005	User Session	To the box connections failures

Syslog ID	Syslog Category	Purpose of syslog messge
710003	User Session	Represents denied connections to the box.
746012, 746013	User Session	Critical AnyConnect

Related Information:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Searching for and Filtering Events in the Event Logging Page

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. CDO 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 CDO 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 CDO Support. That ID is found on the Secure Connectors page in CDO. To find the SEC ID:

1. From the CDO 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:

- About Security Analytics and Logging (SAL SaaS) for the ASA
- Install a Secure Event Connector on an SDC Virtual Machine, on page 371
- 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 388
- 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 CDO 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 380
- Installing an SEC Using a CDO Image, on page 374
- Install a Secure Event Connector on an AWS VPC Using a Terraform Module, on page 388

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. CDO 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 CDO 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 CDO Image, on page 374 or Install an SEC Using Your VM Image, on page 380.

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 CDO, and on the main navigation bar, choose **Analytics** > **Event Logging** 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 CDO's VM Image, on page 11
  - 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 CDO Connectors Installed on a VM You Created required to allow events to reach it.

- Make sure the SDC is communicating with CDO:
  1. In the left pane, click **Tools & Services** > **Secure Connectors**.
  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.

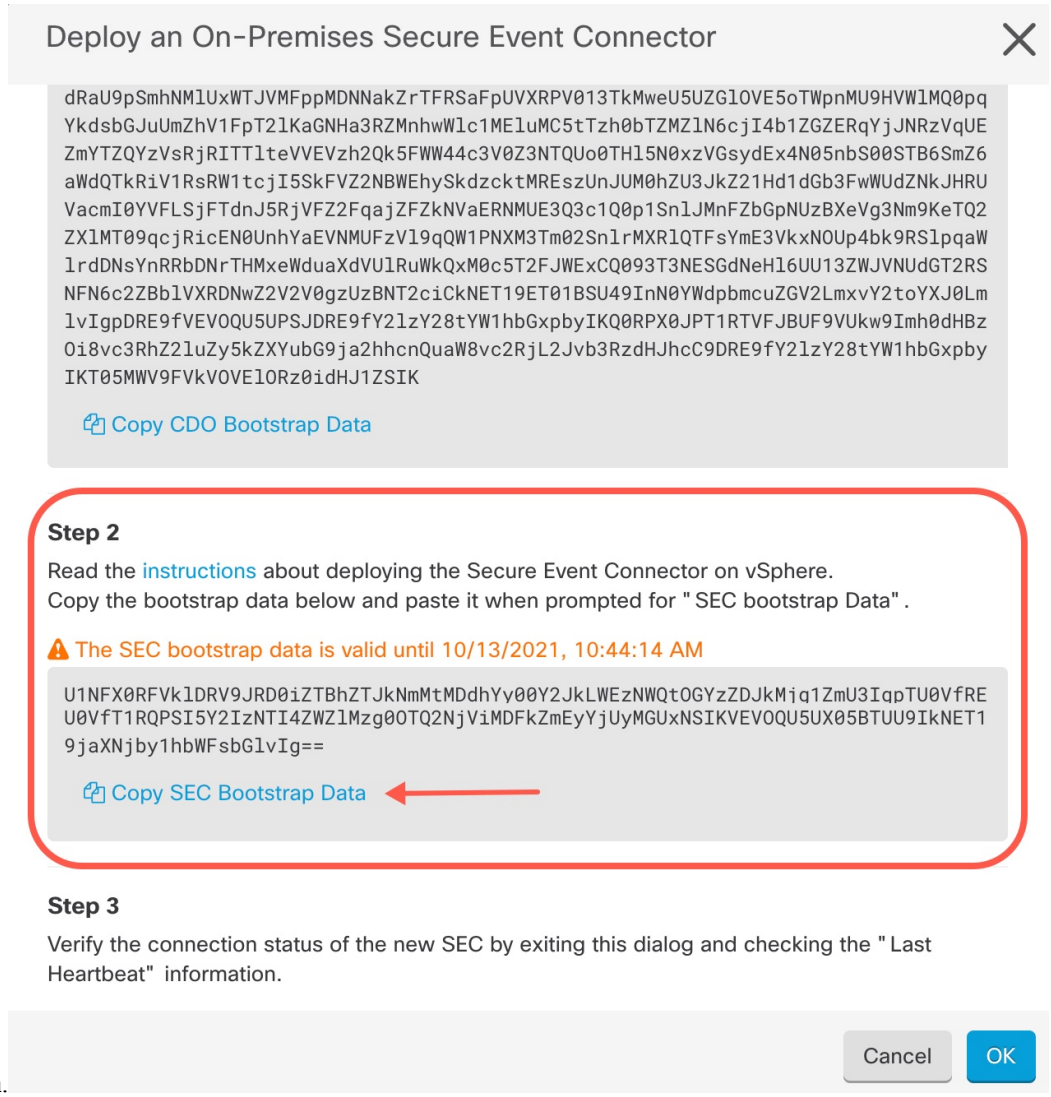
After you have updated the CPU and memory on the VM to accommodate the SEC, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.

Step 1 Log in to CDO.

Step 2 In the left pane, click**Tools & Services** > **Secure Connectors**.

Step 3 Click the blue plus button and 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 ~]$
```

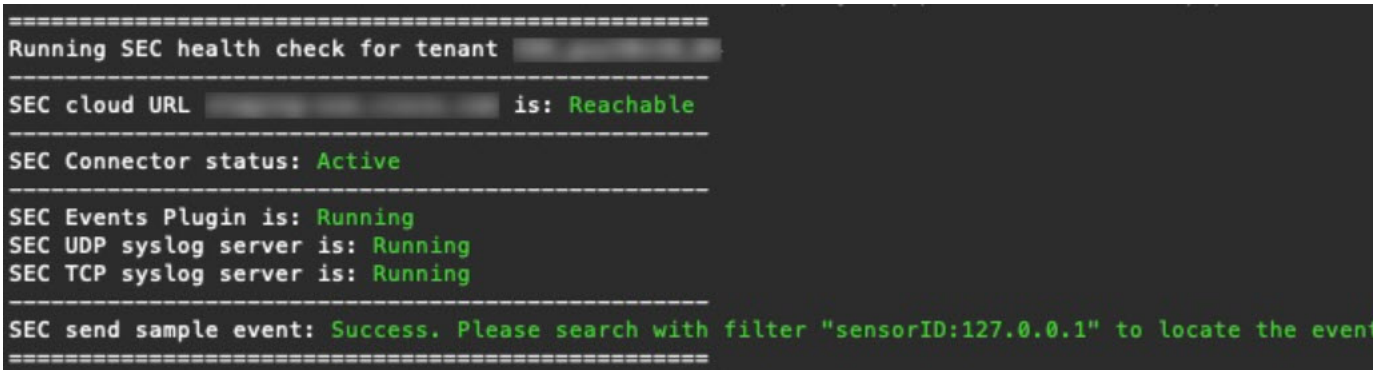
Step 7 At the prompt, run the **sec.sh setup** script:

```
[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 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.

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 CDO Connectors Installed on a VM You Created, on page 385.
- If you installed your SDC using a CDO image, continue to "What to do Next."

What to do next

Return to Implementing Secure Logging Analytics (SaaS) for ASA Devices, on page 345 .

Related Information:

- Troubleshoot a Secure Device Connector, on page 478
- Secure Event Connector Troubleshooting
- Troubleshooting SEC Onboarding Failures
- Troubleshooting Secure Event Connector Registration Failure, on page 488

Installing an SEC Using a CDO 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 CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image, on page 374
   You need one CDO Connector for every SEC you install. The CDO Connector is different than a Secure Device Connector (SDC).
2. Install the Secure Event Connector on your CDO Connector Virtual Machine, on page 386.

Note If you want to create a CDO Connector by creating your own VM, see Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created.

What to do next:

Continue with Install a CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image, on page 374

Install a CDO Connector, to Support a Secure Event Connector, Using a CDO 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 CDO, and on the main navigation bar, choose **Analytics** > **Event Logging** and click **Request Trial**.
- CDO requires strict certificate checking and does not support Web/Content Proxy inspection between the CDO Connector and the Internet. If using a proxy server, disable inspection for traffic between the CDO Connector and CDO.
- **The** CDO **Connector installed in this process must have full outbound access to the Internet on TCP port 443.**
- **Review** Connect CDO to your Managed Devices **to ensure proper network access for the** CDO **Connector.**
- CDO supports installing its CDO Connector VM OVF image using the vSphere web client or the ESXi web client.
- CDO does not support installing the CDO Connector VM OVF image using the VM vSphere desktop client.
- ESXi 5.1 hypervisor.

- System requirements for a VM intended to host only a CDO 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 CDO Connector VM.
  - 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 CDO 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.

Step 1 Log on to the CDO tenant you are creating the CDO Connector for.

Step 2 In the left pane, click **Tools & Services** > **Secure Connectors**.

Step 3 Click the blue plus button and click **Secure Event Connector**.

Step 4 In Step 1, click **Download the** CDO **Connector VM image**. This is a special image that you install the SEC on. Always download the CDO 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:

- 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 VM vSphere desktop client.

Step 7 Deploy the on-premises CDO 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 CDO Connector VM.

Step 10 Login as the CDO 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 CDO 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 CDO user.

Step 15 Follow the prompts to enter your Cisco Defense Orchestrator domain information.

Step 16 Enter the static IP address you want to use for the CDO Connector VM.

Step 17 Enter the gateway IP address for the network on which the CDO Connector VM is installed.

Step 18 Enter the NTP server address or FQDN for the CDO 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 CDO Connector by logging in as the CDO user.

Step 23 At the prompt type **`sudo sdc-onboard bootstrap`**

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

Step 24 When prompted, enter the CDO user's password.

Step 25 When prompted, return to CDO and copy the CDO bootstrap data, then paste it into your SSH session. To copy the CDO bootstrap data:

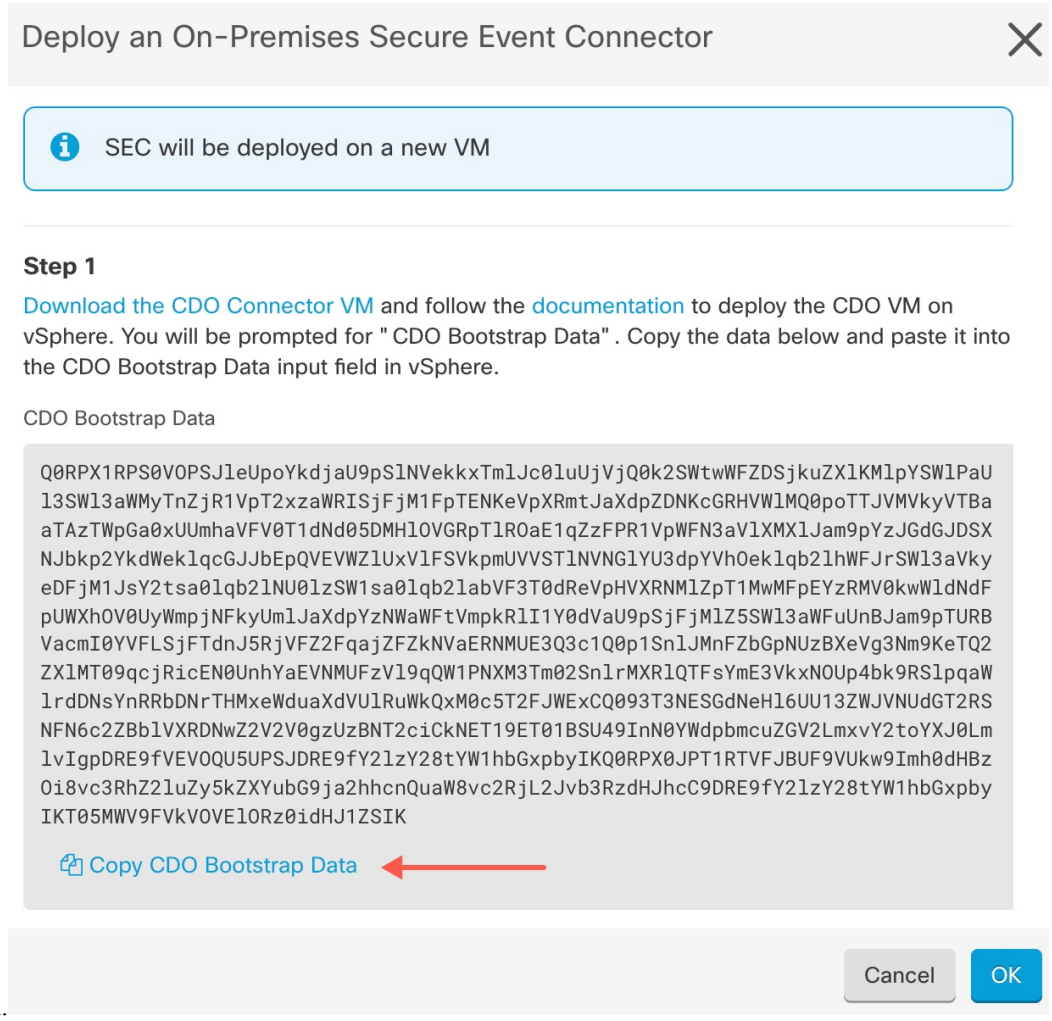
a. Log into CDO.

b. In the left pane, click **Tools & Services** > **Secure Connectors**.

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 CDO 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 CDO 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 CDO Connector VM, on page 377.

Install the Secure Event Connector on the CDO Connector VM

Before you begin

You should have installed CDO Connector VM as described inInstall a CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image, on page 374 .

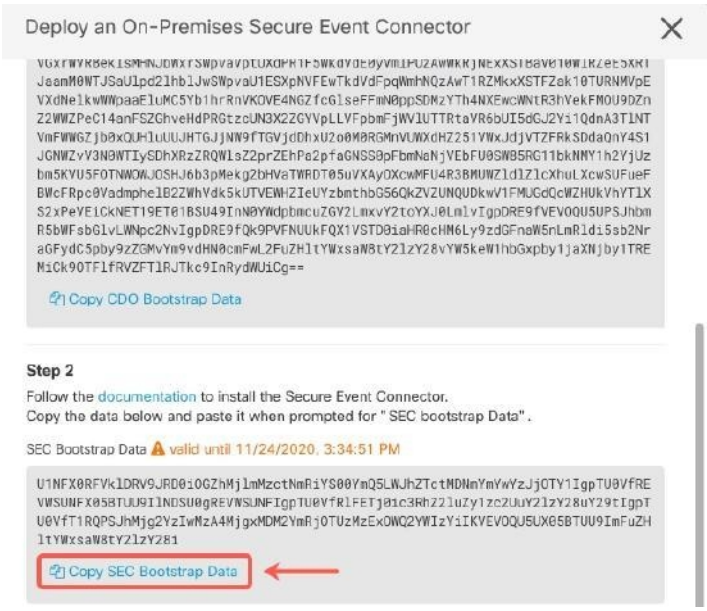
Step 1 Log in to CDO.

Step 2 In the left pane, choose **Tools & Services** > **Secure Connectors**.

Step 3 Select the CDO 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 CDO Connector and log in as the CDO user.

Step 7 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 ~]$
```

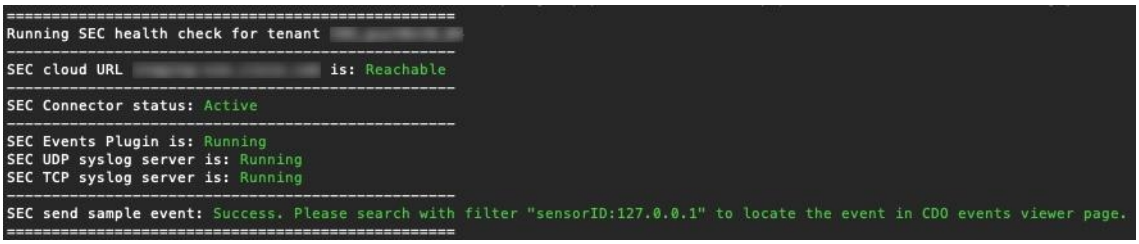
Step 8 At the prompt, run the sec.sh setup script:

```
[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 486.

If you receive the success message return to CDO and click **Done on the Deploy an ON-Premise Secure Event Connector** dialog box.

Step 10 Continue to "**What to do next.**"

What to do next

Return to Implementing Secure Logging Analytics (SaaS) for ASA Devices, on page 345 .

Related Information:

- Troubleshoot a Secure Device Connector, on page 478
- Secure Event Connector Troubleshooting, on page 485
- Troubleshooting SEC Onboarding Failures, on page 486

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 19.

Step 1 Log on to CDO.

Step 2 In the left pane, **Tools & Services** > **Secure Connectors**.

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

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 CDO Connector to Support an SEC Using Your VM Image, on page 380
2. Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 385
3. Install the Secure Event Connector on your CDO Connector Virtual Machine

Note Using a CDO VM image for the CDO Connector is the easiest, most accurate, and preferred method of installing a CDO connector. If you want to use that method, see Installing an SEC Using a CDO Image, on page 374.

What to do next:

Continue to Install a CDO Connector to Support an SEC Using Your VM Image, on page 380

Install a CDO Connector to Support an SEC Using Your VM Image

The CDO Connector VM is a virtual machine on which you install an SEC. The purpose of the CDO 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 CDO Connectors Installed on a VM You Created, on page 385
- Install the Secure Event Connector on your CDO 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 CDO, and on the main navigation bar, choose **Analytics** > **Event Logging** and click **Request Trial**.

- CDO requires strict certificate checking and does not support a Web/Content Proxy between the CDO Connector and the Internet.
- **The CDO Connector must have full outbound access to the Internet on TCP port 443.**
- **Review** Connect CDO to your Managed Devices**to ensure proper network access for the CDO 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 CDO 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 CDO 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 CDO Connector.
  - 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 CDO Connector address is on.
  - The FQDN or IP address of your time server.
- The CDO 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.

Step 1 From the Secure Device Connectors page, click the blue plus button and click Secure Event Connector.

Step 2 Using the link provided, copy the SEC Bootstrap Data in step 2 of the "Deploy an On-Premises Secure Event Connector" window.

Step 3 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 4 Once installed, configure basic networking such as specifying the IP address for the CDO Connector, the subnet mask, and gateway.

Step 5 Configure a DNS (Domain Name Server) server.

Step 6 Configure a NTP (Network Time Protocol) server.

Step 7 Install an SSH server on CentOS for easy interaction with CDO Connector's CLI.

Step 8 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 9 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 10 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 11 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 12 Create two users: **CDO** and **sdc.** The CDO 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 CDO Connector docker container.

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

Step 13 Configure the sdc user to use crontab:

```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```

Step 14 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 15 Add the CDO user to the "wheel" group to give it administrative (sudo) privileges.

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

Step 16 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 17 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 16.

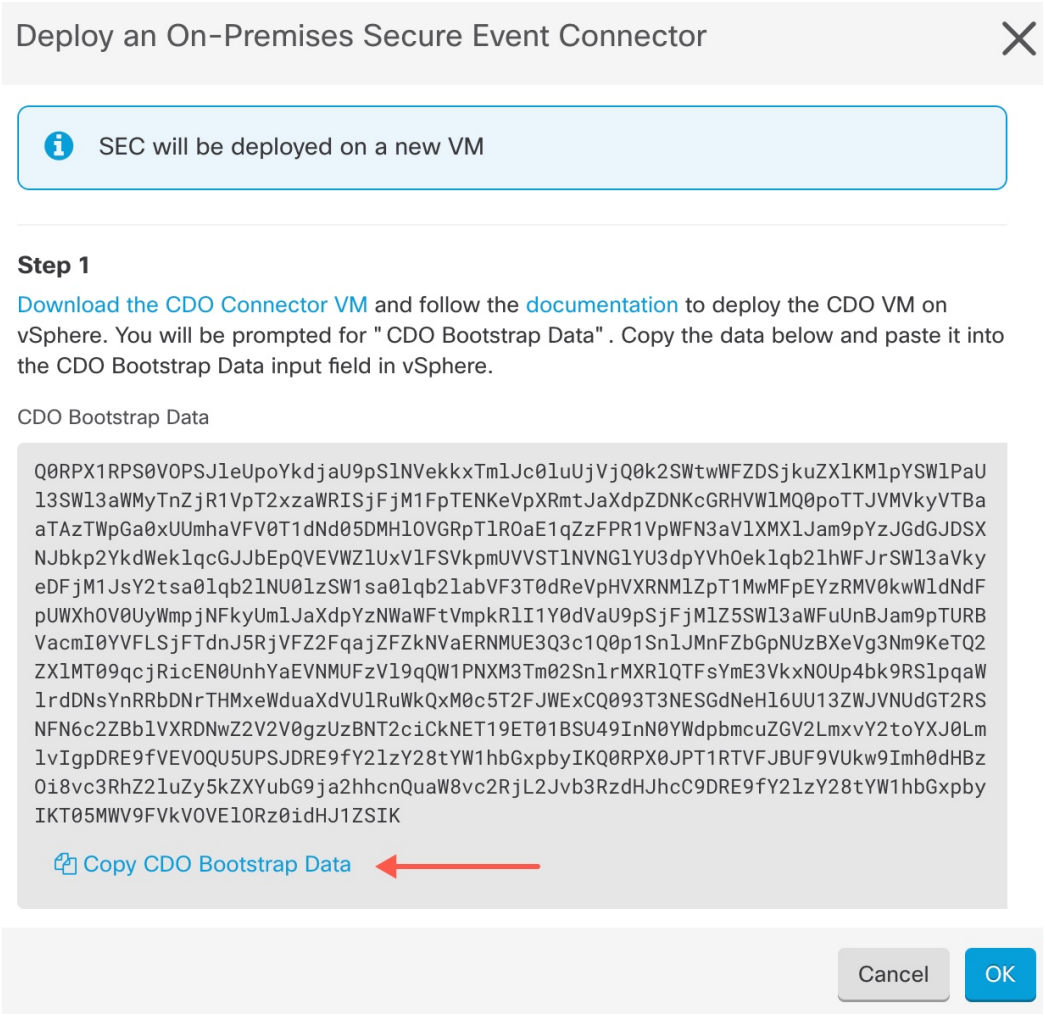
```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

Step 18 If you are currently using a vSphere console session, switch over to SSH and log in as 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 19 Change directories to **/usr/local/**CDO**.**

Step 20 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 21 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_URL>/sdc/bootstrap/CDO_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

Step 22 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 23 Download the bootstrap bundle from CDO.

```
 [sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL" -o $CDO_TENANT.tar.gz

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/CDO_<tenant_name>
```

Step 24 Extract the CDO Connector tarball, and run the bootstrap_sec_only.sh file to install the CDO Connector 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_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/CDO/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/CDO/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/CDO/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/CDO/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

What to do next

Continue to Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 385 .

Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created

If you installed your CDO Connector on your own CentOS 7 virtual machine, you need to 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 386. 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 install and configure your SEC. If you have not already, complete Install a CDO Connector to Support an SEC Using Your VM Image, on page 380 before making these configuration changes.

After you complete one of the additional configuration changes described here, complete Install the Secure Event Connector on your CDO Connector Virtual Machine

Disable the firewalld service on the CentOS 7 VM

1. Log into the CLI of the SDC VM as the "CDO" 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 **CDO** user:

```
[CDO@SDC-VM ~]$ sudo systemctl stop firewalld
CDO@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Restart the Docker service to re-insert Docker-specific entries into the local firewall:

```
[CDO@SDC-VM ~]$ sudo systemctl restart docker
```

4. Continue to Install the Secure Event Connector on your CDO 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 "CDO" 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 **CDO** user. Here is an example of the commands. You may need to specify different port values.

```
[CDO@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
CDO@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[CDO@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:

```
[CDO@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. Continue to Install the Secure Event Connector on your CDO Connector Virtual Machine.

Install the Secure Event Connector on your CDO Connector Virtual Machine

Before you begin

This is the third of three steps you need to complete in order install and configure your Secure Event Connector (SEC). If you have not already, complete these two task before continuing with this procedure:

- Install a CDO Connector to Support an SEC Using Your VM Image, on page 380
- Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 385

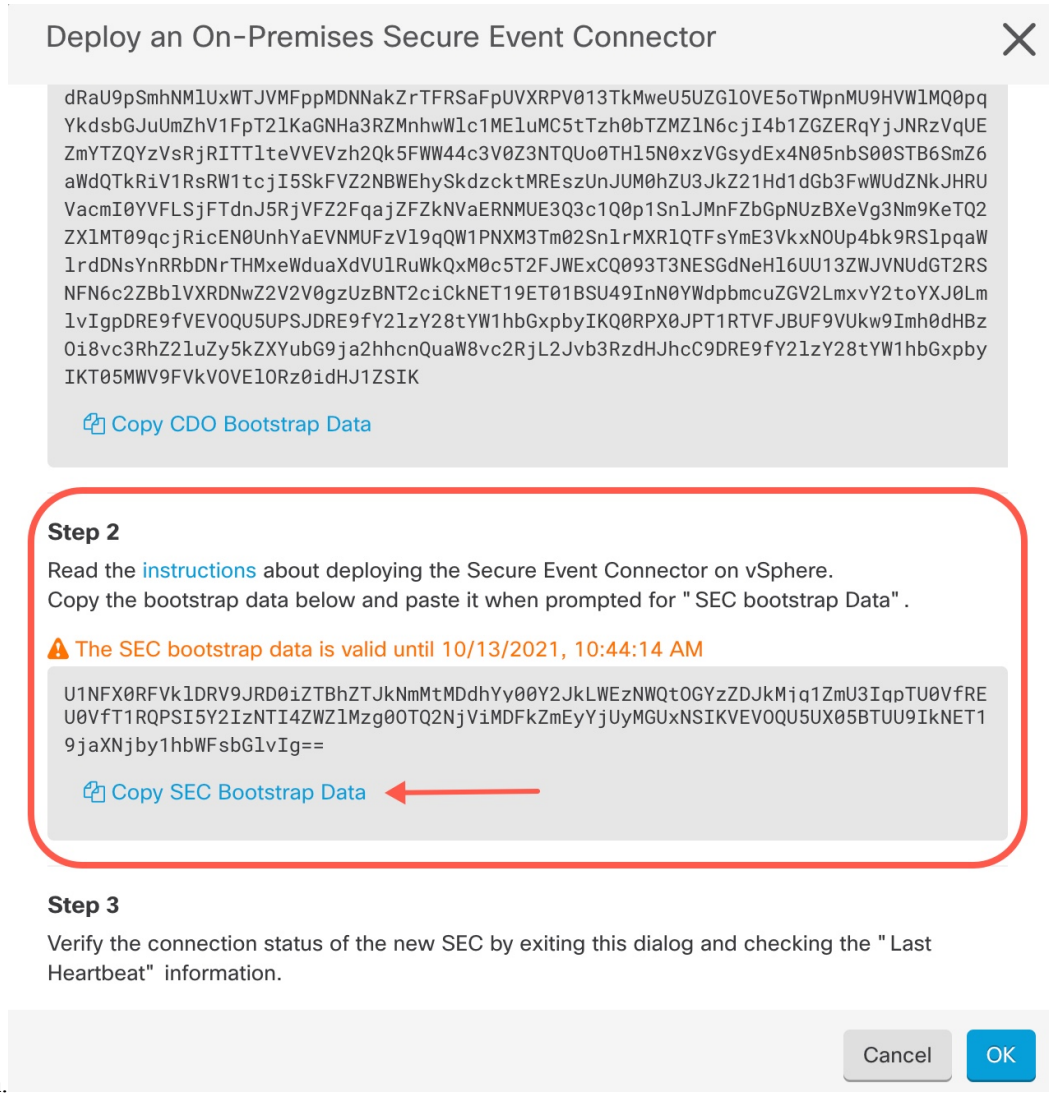
Step 1 Log in to CDO.

Step 2 In the left pane, **Tools & Services** > **Secure Connectors**.

Step 3 Select the CDO Connector that you installed using the procedure in the prerequisites above. In the Secure Connectors table, it will be called a 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 CDO user.

Step 7 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 ~]$
```

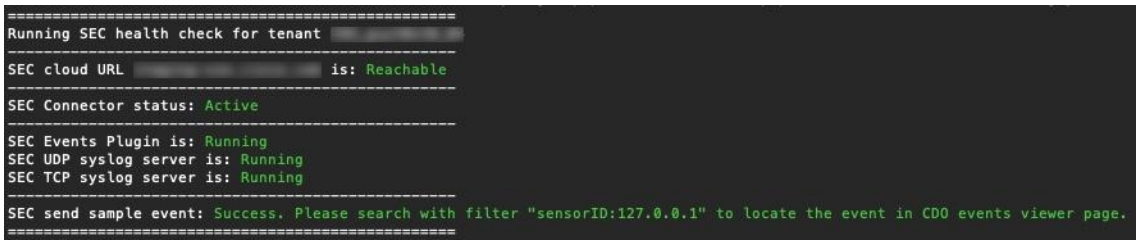
Step 8 At the prompt, run the sec.sh setup script:

```
[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.

Step 10 Continue to "**What to do next**."

What to do next

Return to this procedure to continue your implementation of SAL SaaS: Implementing Secure Logging Analytics (SaaS) for ASA Devices, on page 345 .

Related Information:

- Troubleshoot a Secure Device Connector, on page 478
- 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 CDO 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 371.
- When installing the SEC, make sure you take a note of the CDO bootstrap data and SEC bootstrap data.

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 CDO 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 CDO 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 CDO 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 CDO 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 CDO.
2. Remove SEC files from the SDC.

What to do next: Continue to Remove an SEC from CDO

Remove an SEC from CDO

Before you begin

See Remove the Secure Event Connector, on page 390.

Step 1 Log in to CDO.

Step 2 In the left pane, choose **Tools & Services** > **Secure Connectors**.

Step 3 Select the row with the device type, **Secure Event Connector**.

Warning: Be careful. Do NOT select your Secure Device Connector.

Step 4 In the **Actions** pane, click **Remove**.

Step 5 Click **OK** to confirm your intent to delete the Secure Event Connector.

What to do next

Continue to Remove SEC files from the SDC, on page 390.

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 390 before you begin.

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 CDO_ 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 CDO 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 CDO portal.

Otherwise, you can request a new Secure Cloud Analytics portal from the CDO 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.

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 CDO 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 CDO, on page 393 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 CDO integration or sensor health from the Secure Cloud Analytics portal UI, see Review Sensor Health and CDO Integration Status in Secure Cloud Analytics, on page 392 for

more information. If you want to work with alerts in the Secure Cloud Analytics portal, see Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 393 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 392 for more information.

Review Sensor Health and CDO 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 CDO integration status and your configured sensors from the Sensor List page. The CDO 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 CDO if configured
- yellow cloud icon ( ) - connectivity established with some sensors, or CDO if configured, and one or more sensors is not configured properly
- red cloud icon ( ) - connectivity lost with all configured sensors, and CDO if configured

Per sensor or CDO integration, a green icon signifies connectivity established, and a red icon signifies connectivity lost.

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 CDO.

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 CDO, on page 393.

Viewing Cisco Secure Cloud Analytics Alerts from CDO

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 CDO portal UI. You can cross-launch from CDO 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 CDO, 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 CDO to Secure Cloud Analytics.

To invite other users to your Secure Cloud Analytics portal by email:

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 CDO to Secure Cloud Analytics

To view security alerts from CDO:

Step 1 Log into the CDO 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 CDO, 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 CDO, 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 396
2. Snooze alerts for later analysis, on page 397
3. Update the alert for further investigation, on page 397
4. Review the alert and start your investigation, on page 398
5. Examine the entity and users, on page 400
6. Remediate issues using Secure Cloud Analytics, on page 400
7. Update and close the alert, on page 401

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 CDO for more information on cross-launching from CDO 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:

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:

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:

SUMMARY STEPS

1. From the alert detail, click the arrow icon (➔) next to an observation type to view all logged observations of that type.
2. Click the arrow icon (➔) next to **All Observations for Network** to view all logged observations for this alert's source entity.

DETAILED STEPS

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:

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, CDO 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 CDO Events viewer:

Step 1 In the left pane, choose **Analytics** > **Event Logging**.

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 402
- View Historical Events, on page 403
- Customize the Events View, on page 404

Play/Pause Live Events

You can "play" or "pause" live events as they stream in. If live events are "playing," CDO displays events that match the filtering criteria specified in the Events viewer in the order they are received. If events are paused, CDO does not update the Live events page until you restart playing live events. When you restart playing events, CDO 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.

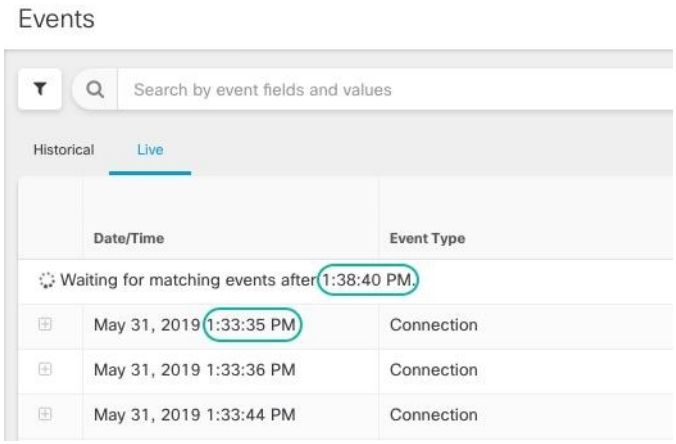
To view all the events that CDO received whether you played or paused live event streaming, click the Historical tab.

Auto-pause Live Events

After displaying events for about 5 consecutive minutes, CDO 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 CDO 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:

Step 1 In the navigation pane, choose **Analytics** > **Event Logging**.

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

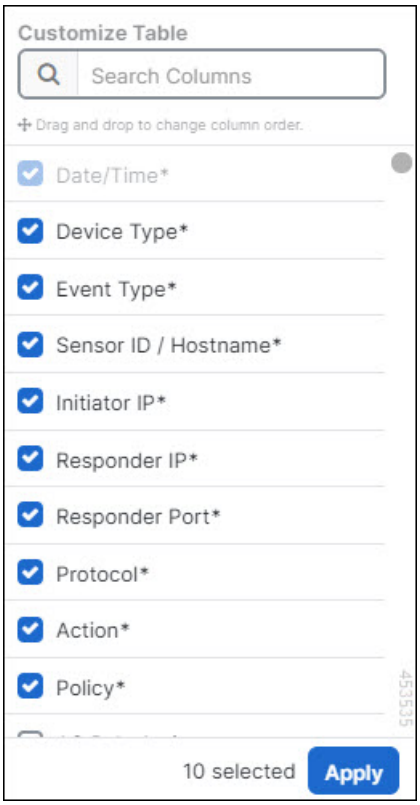
Any changes made to the Event Logging page are automatically saved for when you navigate away from this page and come back at a later time.

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 5: 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 Events view. Click the column filter icon  located to the right of the columns to expand the list of selected columns and manually drag and drop the columns into the order you want, where the column at the top of the list in the drop-down menu is the left-most column in the Event View.

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 CDO **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 CDO 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 CDO Column Name

CDO 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

CDO Column Name	FTD Event Field
NAT Source Port	NAT_InitiatorPort
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:

Step 1 In the left pane, choose **Analytics** > **Event Logging** .

Step 2 Scroll to the far right of the table and click the **Show/Hide Columns** button ≣.

Step 3 Check the columns you want to see and uncheck the columns you want to hide.

Step 4 Mouse-over the column names in the Show/Hide Columns drop down menu and grab the grey cross to rearrange the column order.

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 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 408
Device Type	ASA (Adaptive Security Appliance) 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 CDO 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 439

Change the Time Zone for the Event Timestamps

Change the time zone display for event timestamps on the CDO **Event Logging** page.

Step 1 From the left pane, choose **Analytics** > **Event Logging**.

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 CDO 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.

Step 1 From the main menu, choose **Analytics** > **Event Logging**.

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 439. 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 406 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 439.

Event Attributes in Security Analytics and Logging

Event Attribute Descriptions

The event attribute descriptions used by CDO are largely the same as what is reported by Firepower Device Manager (FDM) and Adaptive Security Device Manager (ASDM).

- For a complete description of Adaptive Security Appliance (ASA) event attributes, see Cisco ASA Series 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:

- Parsed ASA 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
csd	Secure Desktop	724
cts	Cisco TrustSec	776

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
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
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

EventGroup	EventGroupDefinition	Syslog Message ID Numbers (first 3 digits)
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
109023	AAA auth required
109024	Authorization Failed
109025	Authorization Failed

EventID	EventName
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
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected

EventID	EventName
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
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client

EventID	EventName
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
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error

EventID	EventName
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
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP

EventID	EventName
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
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length

EventID	EventName
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
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped

EventID	EventName
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
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID

EventID	EventName
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
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request

EventID	EventName
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
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match

EventID	EventName
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
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped

EventID	EventName
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
746010	Import user failed
746011	Exceed user limit
746012	User IP add

EventID	EventName
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

EventID	EventName
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
716007	WebVPN Unable to Create
716008	WebVPN Debug

EventID	EventName
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
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied

EventID	EventName
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
722011	WebVPN SVC Message
722012	WebVPN SVC Message

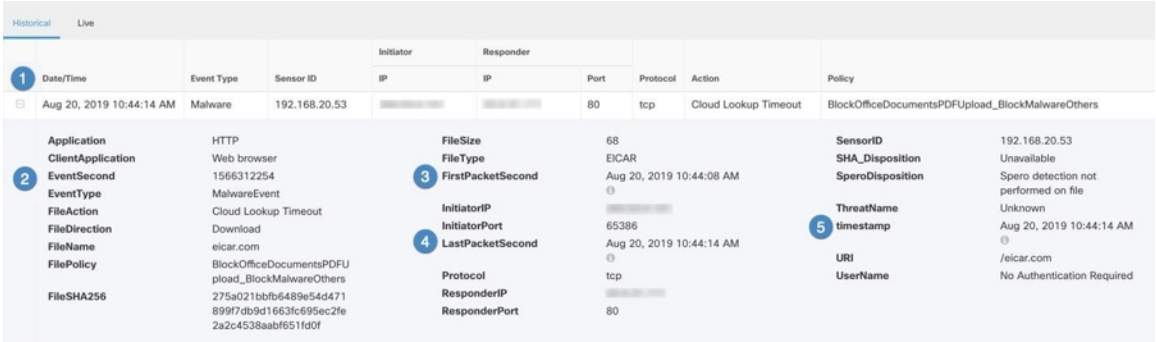
EventID	EventName
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN 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
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address

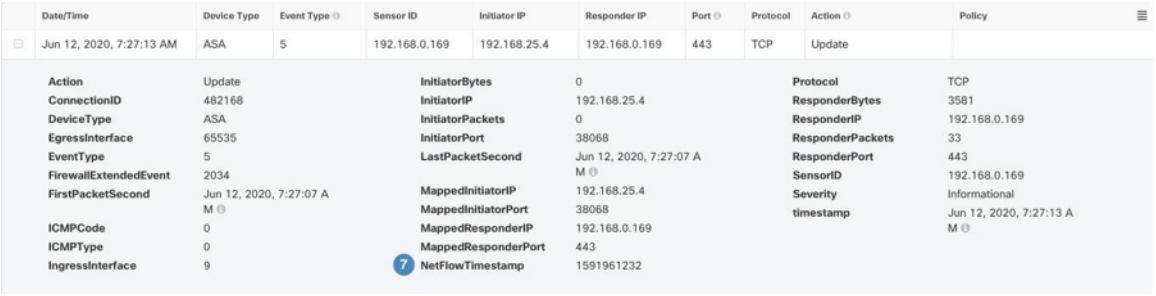
EventID	EventName
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection 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
725005	SSL Server request authentication
725006	SSL Handshake failed

EventID	EventName
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 CDO, 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 CDO, 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 396
2. Snooze alerts for later analysis, on page 397
3. Update the alert for further investigation, on page 397
4. Review the alert and start your investigation, on page 398
5. Examine the entity and users, on page 400
6. Remediate issues using Secure Cloud Analytics, on page 400
7. Update and close the alert, on page 401

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 CDO for more information on cross-launching from CDO 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:

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:

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:

SUMMARY STEPS

1. From the alert detail, click the arrow icon (›) next to an observation type to view all logged observations of that type.
2. Click the arrow icon (›) next to **All Observations for Network** to view all logged observations for this alert's source entity.

DETAILED STEPS

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:

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 CDO. As you add filter criteria, CDO starts to limit what

it displays on the Events 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 447
- Search Historical Events in the Background, on page 446

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 440
- Filter Only NetFlow Events, on page 442
- Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events, on page 442
- Combine Filter Elements, on page 442

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.

Step 1 In the navigation bar, choose **Analytics** > **Event Logging**

Step 2 Click either the Historical or Live tab.

Step 3 Click the filter button . The filtering column can be pinned open by clicking the pin icon .

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 CDO for more information about events.
  - Parsed Events-Parsed ASA Syslog Events contain more event attributes than other syslog events and CDO 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.

- **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.
- **NetFlow**-NetFlow Secure Event Logging (NSEL) for ASA Devices events are different than syslog events. The NetFlow filter searches for all NetFlow events IDs that resulted in an NSEL record. Those "NetFlow event IDs" are defined in the Cisco ASA NetFlow Implementation Guide.

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:

Step 1 From the left menu, choose **Analytics** > **Event Logging**.

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:

Step 1 In the left pane, choose **Analytics** > **Event Logging**.

Step 2 Click the Filter icon and pin the filter open.

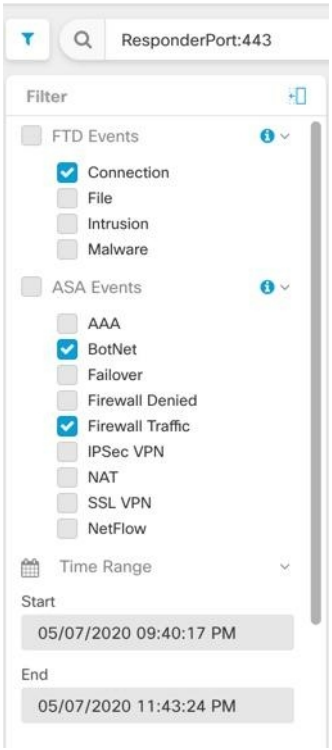
Step 3 Scroll to the bottom of the filter bar and make sure the **Include NetFlow Events** filter is **unchecked**.

Step 4 Scroll back up to the ASA Events filter tree, and make sure the **NetFlow** box is **unchecked**.

Step 5 Pick the rest of your ASA or FTD filter criteria.

Combine Filter Elements

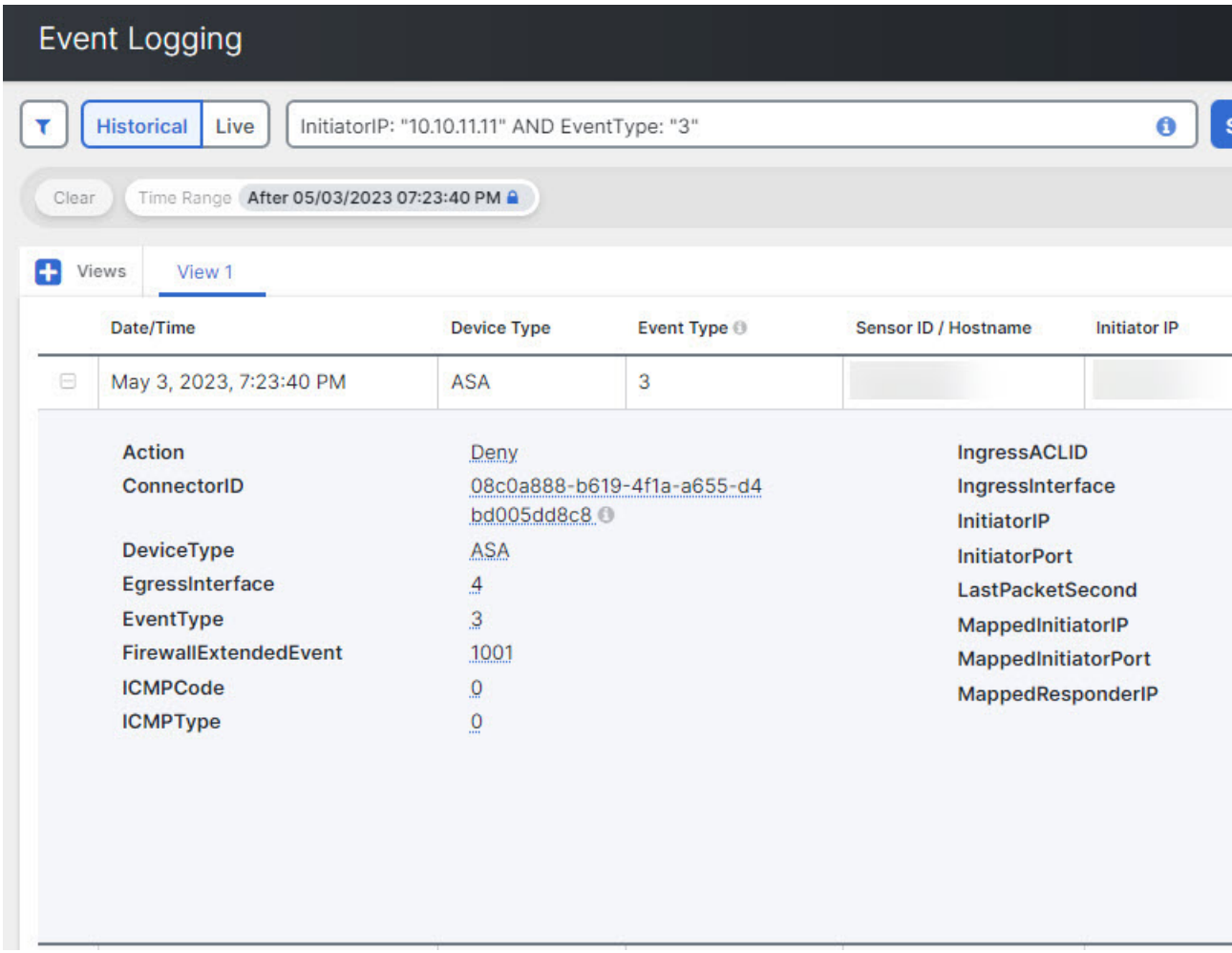
Filtering events generally follows the standard filtering rules in CDO: The filtering categories are "AND-ed" and the values within the categories are "OR-ed." You can also combine the filter with your own search criteria. In the case of event filters; however, the device event filters are also "OR-ed." For example, if these values were chosen in the filter:



With this filter in use, CDO 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

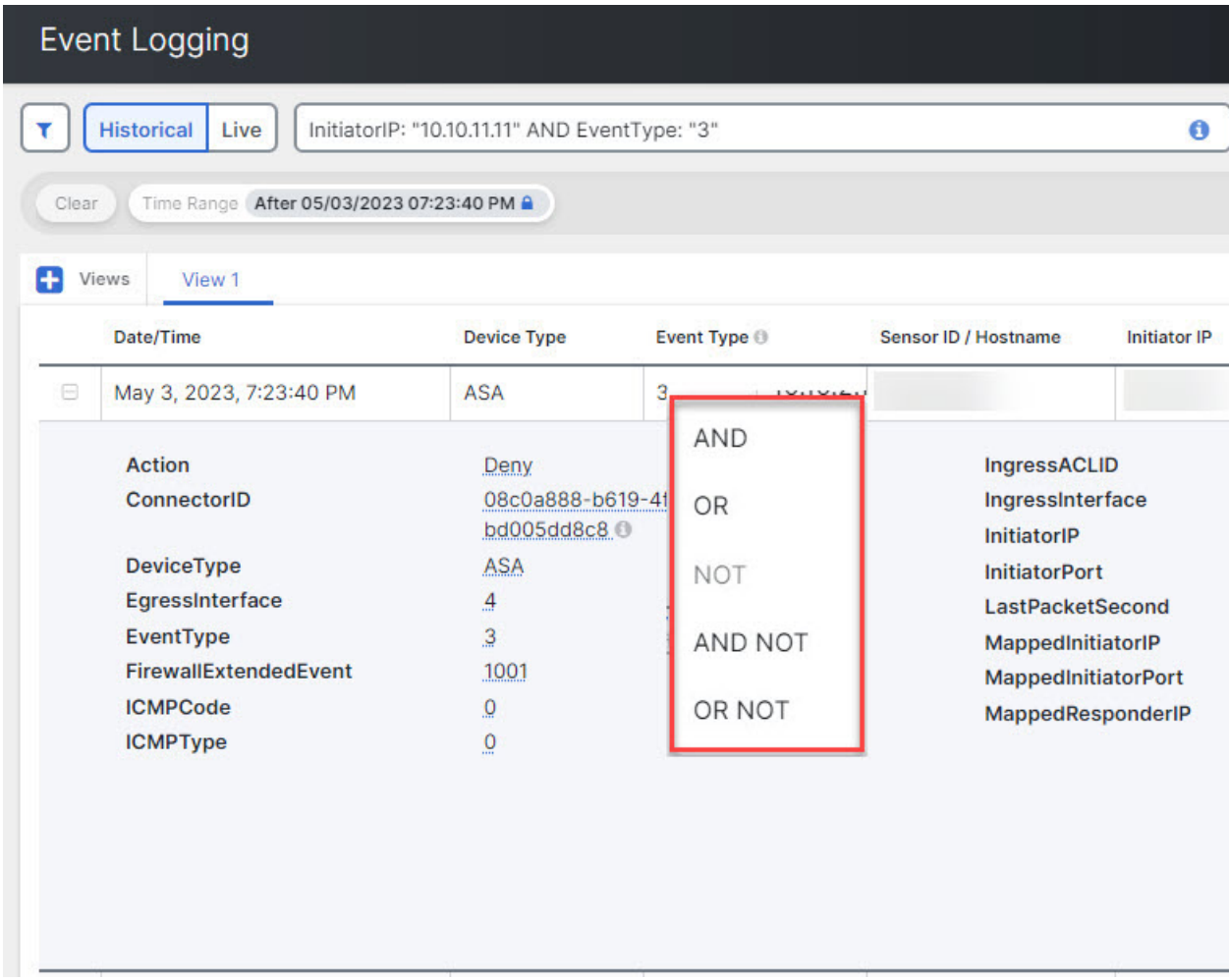
You can search for live or historical events by entering an event attribute and a value in the search field. The easiest way to do this is to click the attribute in the Event Logging table that you want to search for, and CDO enters it in the Search field. The events you can click on will be blue when 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 CDO. 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

CDO 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 Search 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

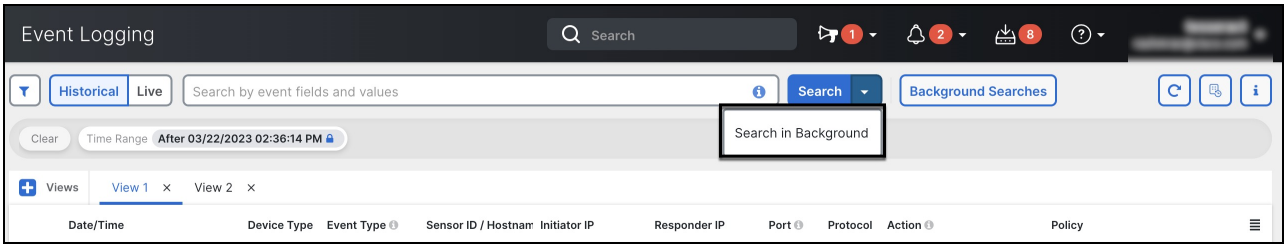
Use the search and background search capabilities to view all logged events in the Event Logging page. Note that background searches can only be performed for historical events.

Step 1 In the navigation bar, choose **Analytics** > **Event Logging**.

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 Aboslute Time Range or Relative Time Range.

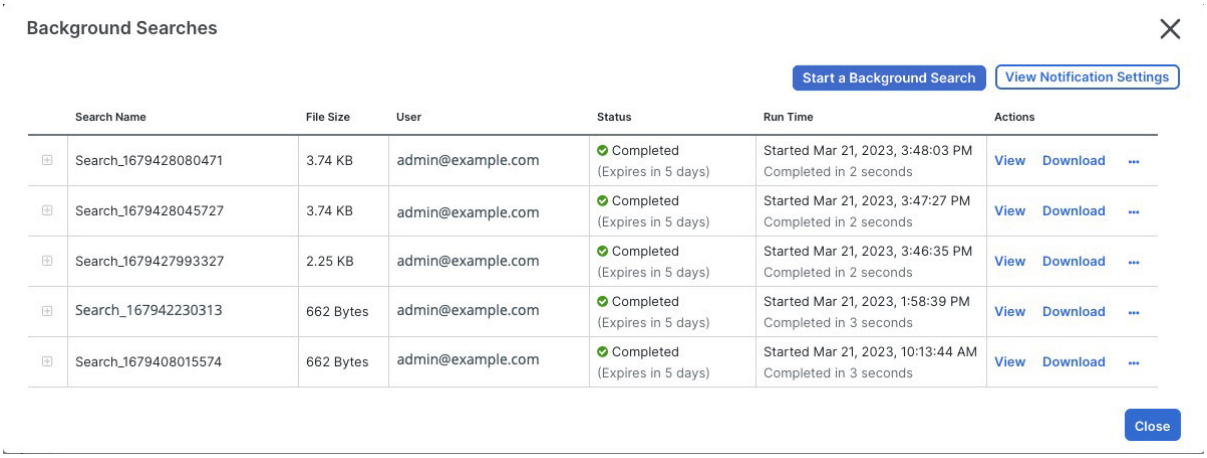
Alternatively, from the **Search** drop-down list, choose **Search in Background** to execute the search in the background while you move away from the search page. You are notified when the search results are ready.



If you click the **Search** button, the results directly appear in the Event Logging view. 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 448 for more information.

Schedule a Background Search in the Event Viewer

Schedule a recurring query in the background in the event viewer page. Searches can only be scheduled for historical events. 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 opt to get alerts on searches that have started, completed, or have failed.

You can schedule a background search only for **historical** events. Use the following steps to create a scheduled background search:

Step 1 In the navigation bar, choose **Analytics** > **Event Logging**.

Step 2 Click the **Historical** toggle to select it. You can only schedule a background search for 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** checkbox 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. Select **Schedule and Search Now**. Alternatively, if you did not opt for the search to start immediately, the button reads **Schedule Search**

What to do next

Results from a scheduled background search are available for review for up to 7 days before CDO automatically deletes them.

Download a Background Search

Search results and schedules qeuries are stored for seven days before CDO automatially removes them. Download a .CSV copy of the background search that was performed for histroical events.

Step 1 In the left pane go to **Analytics** > **Event Logging**.

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 .CSV file automatically downloads to your 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.

If you decide in the middle of your license term to extend your rolling event storage or increase the amount of event cloud storage, you can:

Step 1 Log in to your account on Cisco Commerce.

Step 2 Select your Cisco Defense Orchestrator PID.

Step 3 Follow the prompts to upgrade the length or capacity of your storage capacity.

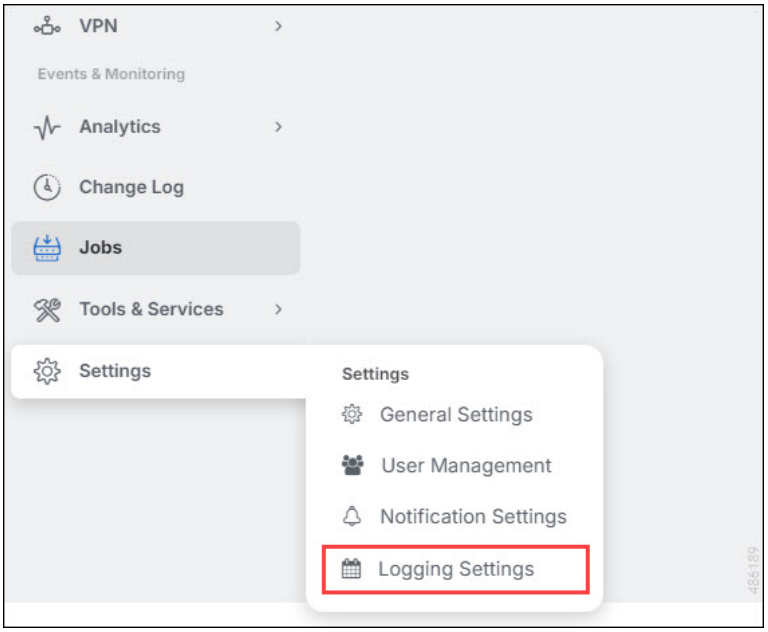
The increased cost will be pro-rated based for the term remaining on your existing license. See the Secure Logging Analytics (SaaS) Ordering Guide for detailed instructions.

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:

Step 1 From the left navigation bar, click **Settings** > **Logging Settings**.

Figure 6: Logging 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

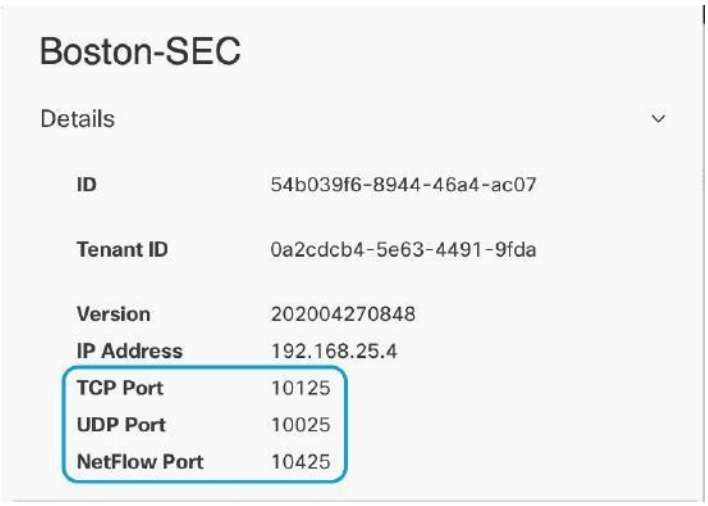
If those ports are already in use, before you configure Secure Logging Analytics (SaaS), look at your SEC device details to determine what ports it is actually using to receive events.

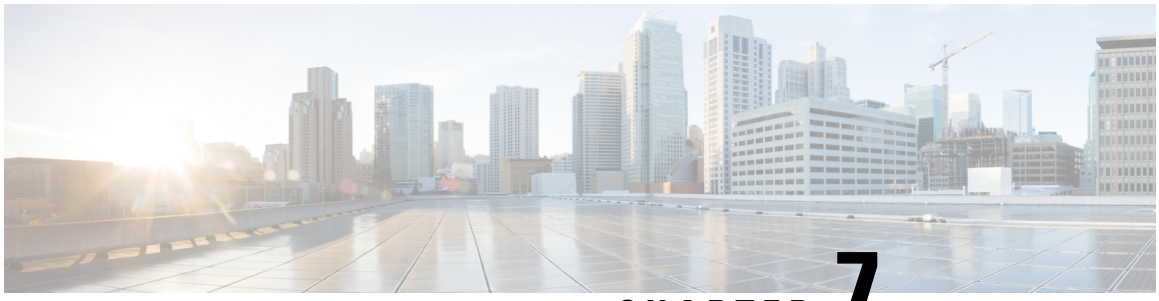
To find the port numbers the SEC uses:

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

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.


Boston-SEC
Details
ID
54b039f6-8944-46a4-ac07
Tenant ID
0a2cdcb4-5e63-4491-9fda
Version
202004270848
IP Address
192.168.25.4
TCP Port
10125
UDP Port
10025
NetFlow Port
10425



CHAPTER 7

Securely Connecting Customers to the Cisco Secure Internet Gateway (SIG)

Managing Umbrella with Cisco Defense Orchestrator

Umbrella is Cisco's cloud-based Secure Internet Gateway (SIG) platform that provides you with multiple levels of defense against internet-based threats. Umbrella integrates secure web gateway, firewall, DNS-layer security, and cloud access security broker (CASB) functionality to protect your systems against threats. By utilizing SIG and DNS protection, the ASA devices are protected with both the local DNS inspection policy on your device and the Umbrella cloud-based DNS inspection policy. By providing several ways to inspect and detect incoming traffic, Umbrella makes the ASA device comparable to FTD next-generation firewall (NGFW).

At this time, CDO only supports ASA integration with an Umbrella organization.

Build a Bridge with SASE

Secure Access Service Edge (SASE) is a forward-thinking framework in which networking and security functions converge into a single integrated service that works at the cloud edge to deliver protection and performance. This effort provides a way to consolidate services safely and securely, regardless of your location, and allows you to control and manager your network no matter the size of your organization. Reduced complexity and an agile take of management means your deployments are simple, scalable, and and secure.

What is an Umbrella Organization?

An Umbrella organization is a group of users with varying user roles that are associated with a single license key; a single user can have access to multiple Umbrella organizations. Every Umbrella organization is a separate instance of Umbrella and has its own dashboard. Organizations are identified by their name and their organization ID (Org ID). The Org ID is used to identify your organization for deploying components such as virtual appliances, and sometimes support may request your Org ID.

What is a SIG Tunnel?

A Secure Internet Gateway (SIG) tunnel is an instance of a SIG IPSec (Internet Protocol Security) tunnel that occurs between the ASA and Umbrella, where all internet-bound traffic is forwarded to Umbrella SIG for

inspection and filtering. This solution provides centralized management for security so network administrators do not have to separately manage security settings for each branch.

When you onboard an Umbrella organization that has tunnels configured, these tunnels are listed in CDO's Site-to-site VPN page. To create a SASE tunnel for your Umbrella organization from the CDO UI, see Configure a SASE Tunnel for Umbrella.

Note If you onboard an Umbrella organization and its peer devices, the Site-to-site VPN page combines all the devices to the tunnel associated with that organization into a single entry. To manually refresh the Tunnels page and read in any changes made from the Umbrella dashboard, see Read Umbrella Tunnel Configuration.

How does CDO Communicate with Umbrella?

You must onboard the Umbrella organization as well as any ASA devices associated with the organization.

When an ASA device is associated with an Umbrella cloud, the connection requires a site-to-site VPN SIG tunnel to create a secure connection between the device and the cloud. CDO communicates with both the Umbrella organization and the ASA devices. This dual-communication method allows CDO to instantly detect changes in configuration or tunnel changes, and immediately alert you to an out-of-bound changes, errors, or unhealthy states for Umbrella, the ASA, and the tunnels.

When you onboard an Umbrella organization to CDO, you onboard with the organization's API key and Secret, both of which are unique to the organization and the ASA devices associated with that organization. CDO communicates to the Umbrella cloud with the Umbrella API, using the API key and Secret used to onboard the organization to request and send information about the ASA devices. This level of communication does not compromise the SIG tunnel that exists between the ASA and the Umbrella cloud.

Once an Umbrella organization is onboarded, the **Inventory** page displays any detected ASA devices associated with the org as "peers", and notes whether the devices are onboarded to CDO or not. If a peer device is not already onboarded, you have the option to onboard directly from that page by clicking Onboard Device. When an ASA device that is associated with an Umbrella organization is onboarded to CDO, the **Inventory** page displays the relationship and the VPN Tunnels page shows the tunnels between the device and the organization. If an ASA device that is associated with an organization is not onboarded to CDO, the tunnels associated with the device are displayed in the VPN Tunnels and you can opt to onboard the device directly from this page.

How do I access the Umbrella Cloud from CDO?

Once the Umbrella organization is successfully onboarded onto CDO, you can cross-launch to the organization's dashboard or to the Umbrella Tunnels page from the CDO UI.

See Cross-launch to the Umbrella dashboard, on page 458 and Cross-launch to the Umbrella Tunnels Page, on page 459 to access the Umbrella Cloud from the CDO UI.

Prerequisites

Supported Hardware and Software

Umbrella organizations are cloud-based and thusly version-less. Note that when you onboard an Umbrella organization to CDO, you are only able to associate that organization with an ASA device.

For Umbrella integration, CDO supports ASA devices running 9.1.2 and later. See Cloud Device Support Specifics, on page 41 for a list of ASA device models and software that CDO supports.

Licensing Requirements

In order to successfully onboard an Umbrella organization to CDO, you must have one of the following license packages selected:

- Umbrella SIG Essentials
- SIG Advantage

Onboarding

To successfully manage an Umbrella account, you must onboard both the Onboarding an Umbrella Orgnization and the Onboard ASA Device to CDO associated with it. Once you onboard an Umbrella organization, CDO reads any existing ASA tunnels associated with the organization and monitor the health status of these tunnels as well as any additional tunnels you create and associate with the organization. Before you onboard an Umbrella organization, review the general device requirements and onboarding prerequisites.

If you happen to onboard an Umbrella organization before onboarding any ASA devices associated with it, you can view the ASA peer from the **Site-to-site VPN** page and onboard the device from the VPN page.

Note If you have an ASA pair configured for failover, you must **only** onboard the active device of the two peers. Onboarding both the active and the standby devices to CDO may generate duplicate tunnel information for SASE tunnels that are already configured in Umbrella.

Monitoring Your Network

CDO provides reports summarizing the impact of your security policies and methods of viewing notable events triggered by those security policies. CDO 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 commit in CDO with a help ticket or other operational request.

Change Log

The Manage Change Logs in CDO continuously captures configuration changes as they are made in CDO. This single view includes changes across all supported devices and services. Because Umbrella is a cloud-based product, changes are immediately deployed.

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 CDO.
- 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.

Note Note that when you create, edit, or delete a SASE tunnel associated with an Umbrella organization, the request and configuration changes appear for the Umbrella organization and any ASA device associated with it.

Umbrella Documentation

- Umbrella Help
- Umbrella and Cisco ASA Configuration
- Connect to Cisco Umbrella Through Tunnel
- Cisco Umbrella API

Onboarding an Umbrella Organization

Umbrella License Requirements

In order to successfully onboard an Umbrella organization to CDO, you must have one of the following license packages selected from the Umbrella dashboard:

- Umbrella SIG Essentials
- SIG Advantage

To verify the licenses that are currently enabled, log into the Umbrella dashboard and navigate to **Admin** > **Licensing**.

Generate an API Key and Secret

Generate a new API key and retrieve **both** the **API Key** and the corresponding **Secret** before you onboard an Umbrella organization to CDO.

If you do not currently have an API key, use the following procedure to create one:

Before you begin

The management API key from Umbrella is used for the following Umbrella services:

- Networks and Domains
- Network Tunnels
- Users and Roles
- Destination Lists
- Service Providers

You cannot onboard an Umbrella organization without allowing CDO access to these services.

Step 1 Access the Cisco Umbrella dashboard and log into your organization.

Step 2 In the Umbrella dashboard, click **Admin** in the left navigation pane and select **API Keys**.

Step 3 Click **Create API Key**.

If you already have an API key but do not have the secret saved, navigate to the **Admin** > **API Keys**screen and click **Refresh** to update the key and secret.

Step 4 To create a new API key and Secret, click the + button.

Step 5 Enter a **Name** and add the following scopes to the API key:

- Deployments.
- Policies.

Step 6 Click **Generate Key**.

Step 7 Copy the API Key and the corresponding Secret. We recommend temporarily pasting it into a note or .txt file until you are ready to use it.

Umbrella Organization ID

You must use the Umrbrella organization's locate the organization ID and use that along with the login credentials to successfully onboard the organization to CDO:

Step 1 Access the Cisco Umbrella dashboard and log into your organization/

Step 2 The page URL will contain a numeric identifier. For example, the Organization ID for https://dashboard.umbrella.com/o/**123456**/#/overview is **123456**.

Step 3 Copy the Organization ID from the URL. We recommend temporarily pasting it into a note until you are ready to use it.

Onboarding an Umbrella Orgnization

Use the following procedure to onboard an Umbrella organization to CDO:

Before you begin

Read the Umbrella License Requirements, on page 456 before you onboard this environment.

Step 1 In the Umbrella dashboard, locate the Umbrella Organization ID, on page 457 and Generate an API Key and Secret, on page 456. Have these items available during this procedure.

Step 2 Log into CDO.

Step 3 In the navigation bar, click **Inventory**

Step 4 Click the blue plus button to begin onboarding the device.

Step 5 Click **Umbrella Organization**.

Step 6 Enter the Umbrella Network Device's **API Key** and corresponding **Secret** that you generated from the Umbrella dashboard, and the **Organization ID** from your Umbrella dashboard's URL.

Step 7 Click **Next**.

Step 8 (Optional) Add unique **Labels** for the device. You can later filter your list of devices by this label.

Step 9 Click **Go to Inventory**.

Reconnect an Umbrella Organization to CDO

Warning CDO cannot successfully deploy or read configuration changes to or from an Umbrella organization if the stored credentials are invalid, but CDO may successfully deploy or read changes from any ASA devices associated with the org. This may cause issues once the credentials are updated and validated. We recommend updating the organization credentials prior to deploying any configuration changes.

If the API key and secret to an Umbrella Organization has been refreshed or has timed out, you have to manually reconnect the Umbrella organization to CDO. Use the following procedure to reconnect:

Step 1 Go to the Umbrella Dashboard. Click **Admin** in the left navigation pane and select the existing Umbrella Management **API Keys**.

Step 2 Click **Refresh**. Confirm that you want to refresh the API key and secret.

Step 3 Copy the API Key and the corresponding Secret.

Step 4 Log into CDO.

Step 5 Navigate to the **Inventory** page.

Step 6 Use to the filter or search bar to locate the Umbrella Organization.

Step 7 In the **Device Actions** pane, click **Reconnect**. CDO confirms the stored API Key and secret are no longer valid.

Step 8 Paste the API key and Secret into the appropriate pop-up window.

Step 9 Click **Continue**.

Step 10 Once CDO confirms the new key and secret are valid, click **Close**.

Cross-launch to the Umbrella dashboard

Once the ASA device and the Umbrella organization are successfully onboarded onto CDO, you can cross-launch to the organization's dashboard from the CDO UI.

Use the following procedure to cross-launch to your device's Umbrella dashboard:

Step 1 Log into CDO.

Step 2 Click **Inventory**.

Step 3 Locate, or Filters, for the Umbrella organization.

Step 4 Click **Manage Umbrella Organization** in the Management pane. CDO launched a new tab in your browser that opens to the Umbrella dashboard associated with the selected organization.

Delete a Device from CDO

Use the following procedure to delete a device from CDO:

Step 1 Log into CDO.
Step 2 Navigate to the **Inventory** page.
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.

Configure an Umbrella Organization

Read Umbrella Tunnel Configuration

Once an Umbrella organization is onboarded to CDO, you can manually force CDO to request and update the tunnels configuration from Umbrella. This includes tunnels that were added, deleted, or modified.

Warning If a tunnel is deleted from CDO while the Umbrella organization credentials are considered invalid, or have changed since you onboarded the organization, CDO can only deploy the tunnel configuration to the ASA devices associated with the organization. Upon updating the credentials, CDO reads the Umbrella configuration and repopulates any tunnels that were deleted. Due to the tunnel existing in the Umbrella organization but not any of the ASA devices, there will be a synchronization issue and the ASA devices may not appear as peers to organization.

Step 1 Log into CDO.
Step 2 In the left pane, click **Inventory** > **Devices**.
Step 3 Click the **ASA** tab.
Step 4 Select the Umbrella organization so it is highlighted.
Step 5 Under **Actions**, select **Read Tunnels**.

Cross-launch to the Umbrella Tunnels Page

Once the ASA device and the Umbrella organization are successfully onboarded onto CDO, you can cross-launch to the Umbrellas dashboard for tunnels from the CDO UI.

Use the following procedure to cross-launch to your device's Umbrella tunnels page:

Step 1 Log into CDO.

Step 2 Navigate to the VPN window. Select **Site-to-Site VPN**.

Step 3 Select the desired tunnel so it is highlighted.

Step 4 In the Actions pane, click **Manage Tunnel in Umbrella**. CDO launches a new tab in your browser that opens to the Tunnels overview page.

Configure a SASE Tunnel for Umbrella

Use the following procedure to create a SASE tunnel for an Umbrella organization:

Before you begin

Note that the Umbrella organization and the ASA device you want to create the tunnel for **must** already be onboarded to CDO.

If the ASA or Umbrella organization associated with the tunnel you just deployed is in an unhealthy state, CDO may not be able to successfully deploy the tunnel. If you experience any issues, contact Cisco TAC.

Step 1 Log into CDO.

Step 2 Navigate to the **VPN** window. Select **Site-to-Site VPN**.

Step 3 Click the blue plus button and select **Create SASE Tunnel**.

Step 4 Enter the Umbrella Peer information:

- **Select Umbrella** - Select the **Umbrella** organization of your choice.
- **Datacenter** - Select a head-end datacenter. We recommend selecting a datacenter that is geographically close to the ASA associated with the Umbrella organization.

Step 5 Enter the ASA Peer information:

- **Select ASA Device** - Select an ASA device that is associated with the Umbrella organization from the drop-down list and then click **Select**.
- **Public Facing Interface** - Select an IPv4 address that is static and publicly routable. The address used should not be used for NAT.
- **LAN Address** - Select the LAN interfaces that controls the LAN subnet. You must select at least one interface for LAN.
- **Virtual Tunnel Interface** - This field is automatically filled once you select the Umbrella organization and the ASA peer device. If necessary, you can manually enter an IP address that will be used as the new VTI.

Step 6 The **Passphrase** is automatically filled once you select the Umbrella organization and the ASA peer device. The **Confirm Passphrase** is also automatically filled. You can manually enter these fields if necessary.

Step 7 (Optional) The **Deploy changes to ASA immediately** toggle at the bottom of the pop-up window is enabled by default. When enabled, the SASE tunnel configuration is immediately deployed to the ASA peer selected in the tunnel configuration. If you want to stage changes and deploy later, manually toggle the option to disable.

Step 8 Click **Deploy**. Optionally, click **Deploy and Create Another** to simultaneously deploy this SASE tunnel and create another tunnel. Once deployed, the tunnel will appear in the VPN Tunnels page. If you choose to **Deploy and Create Another SASE tunnel**, CDO saves both the Umbrella organization selection and the **Deploy changes to ASA immediately**

toggle setting and automatically applies these selections to the next tunnel configuration. You can manually alter these selections prior to deploying.

Edit a SASE Tunnel

Use the following procedure to modify an existing SASE tunnel:

Step 1 Log into CDO.

Step 2 Navigate to the **VPN** window. Select **Site-to-Site VPN**.

Step 3 Select the tunnel you want to modify.

Step 4 In the Actions pane, select **Edit**.

Step 5 Edit the following fields of the SASE tunnel:

- **Name** - Change the name of the SASE tunnel as it appears in CDO and the Umbrella dashboard.
- **Umbrella Peer's Datacenter** - Select a new head-end datacenter form the drop-down menu.
- **ASA Peer's Public Facing Interface** - Select a new IPv4 address from the drop-down menu.
- **ASA Peer's LAN Interfaces** - Select one or more new LAN interfaces from the drop-down menu.
- **ASA Virtual Tunnel Interface (VTI) Address** - Manually edit the VTI.
- **Passphrase** - Manually modify the passphrase for the tunnel.
- **Confirm Passphrase** - Manually modify this entry to match the passphrase and confirm the new value.

Step 6 (Optional) The **Deploy changes to ASA immediately** toggle at the bottom of the pop-up window is enabled by default. When enabled, the SASE tunnel configuration is immediately deployed to the ASA peer selected in the tunnel configuration. If you want to stage changes and deploy later, manually toggle the option to disable. If you opt to stage changes and deploy later, the ASA peer status in the **Inventory** page appears as `Deploy Pending`.

Step 7 Select **Save Updates**.

Delete a SASE Tunnel from Umbrella

Use the following procedure to delete a SASE tunnel through the CDO UI:

Before you begin

To delete a SASE tunnel, the ASA associated with it must have a synced status in CDO. You cannot delete a tunnel if the device is uhealthy.

Note that if you delete a SASE tunnel from CDO, the tunnel is removed from both the ASA device and the Umbrella organization associated with it.

Warning If you delete a tunnel from CDO while the Umbrella organization credentials are considered invalid, or have changed since you onboarded the organization, CDO can only deploy the tunnel configuration to the ASA devices associated with the organization. Upon updating the credentials, CDO reads the Umbrella configuration and repopulates any tunnels that were deleted. Due to the tunnel existing in the Umbrella organization but not any of the ASA devices, there will be a synchronization issue and the ASA devices may not appear as peers to organization. We recommend confirming the Umbrella credentials prior to deleting any tunnels associated with the organization.

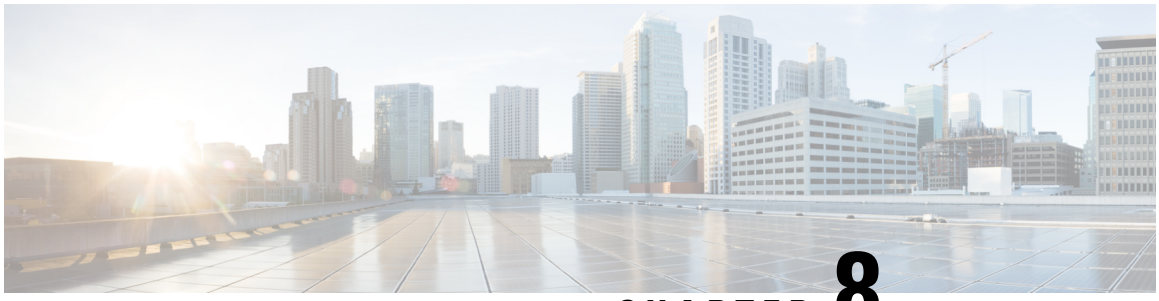
Step 1 Log into CDO.

Step 2 In the left pane, click **VPN** > **Site-to-Site VPN**.

Step 3 Select the tunnel you want to delete from CDO.

Step 4 Under **Actions**, click **Delete**.

Step 5 Confirm you want to delete the tunnel and click **OK**.



CHAPTER 8

Integrating CDO with Cisco Security Cloud Sign On

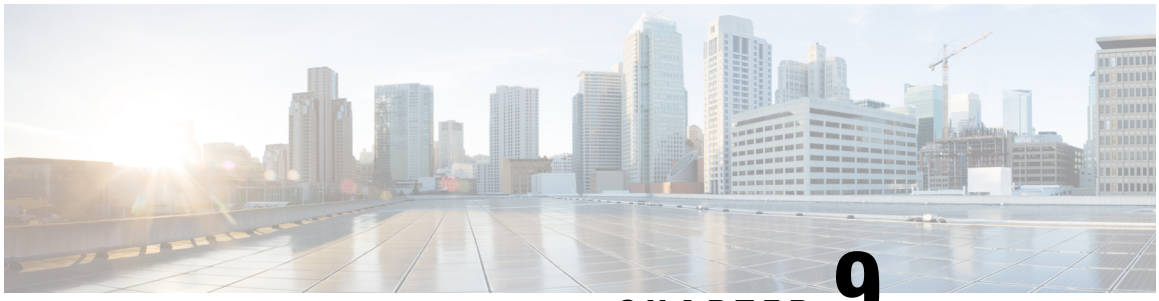
Merge Your CDO and Cisco XDR Tenant Accounts

If your Secure Firewall Threat Defense or On-Prem Firewall Management Center is used with CDO or Cisco Security Analytics and Logging (SaaS) and Cisco XDR, you must link your CDO 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 9

Terraform

About Terraform

CDO customers can use the CDO Terraform provider and CDO Terraform modules to rapidly set up their tenants using code that is repeatable and version-controlled. The CDO 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:

- CDO Terraform Provider page
- CDO SDC on vSphere module page
- CDO SDC on AWS module page
- CDO SEC on AWS module page
- Work through the Devnet learning lab
- Automating Security Infrastructure Management Using the Cisco Defense Orchestrator Terraform Provider - Learning Lab
- CDO automation examples on GitHub

Support

The CDO 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:

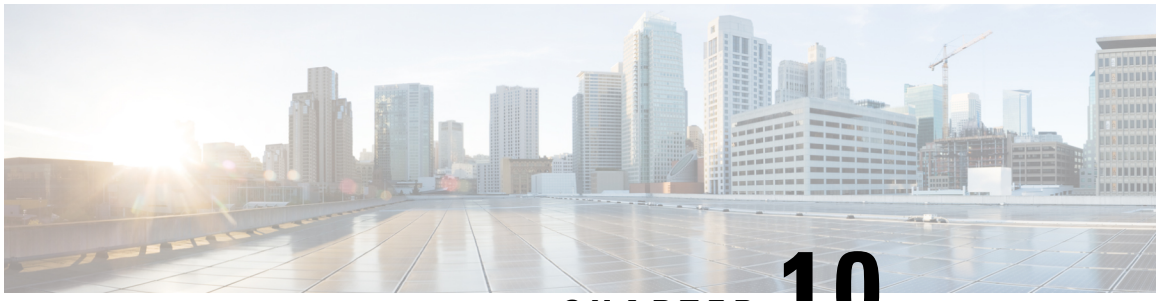
Module	Repository
CDO Terraform Provider	https://github.com/ciscodevnet/terraform-provider-CDO
CDO SDC Module (vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-CDO-sdc
CDO SDC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-CDO-sdc
CDO SEC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-CDO-sec

Contribution to Repositories

The CDO 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 10

Troubleshooting

This chapter covers the following sections:

Troubleshoot an Secure Firewall ASA Device

ASA Fails to Reconnect to CDO After Reboot

If CDO and your ASA do not connect after an ASA reboot, it may be because the ASA has fallen back to using an OpenSSL cipher suite that is not supported by CDO's Secure Device Connector (SDC). This troubleshooting topic tests for that case and provides remediation steps.

Symptoms

- ASA reboots and CDO and the ASA fail to reconnect. CDO displays the message, "Failed to reconnect."
- When attempting to onboard an ASA, CDO displays the message: *Certificate could not be retrieved for <ASA_IP_Address>*.

Cannot onboard ASA due to certificate error

Environment: ASA is configured with client-side certificate authentication.

Solution: Disable client-side certificate authentication.

Details: ASAs support credential-based authentication as well as client-side certificate authentication. CDO cannot connect to ASAs that use client-side certificate authentication. Before onboarding your ASA to CDO, make sure it does not have client-certificate authentication enabled by using this procedure:

Step 1 Open a terminal window and connect to the ASA using SSH.

Step 2 Enter global configuration mode.

Step 3 At the hostname (config)# prompt, enter this command:

```
no ssl certificate-authentication interface interface-name port 443
```

The interface name is the name of the interface CDO connects to.

Determine the OpenSSL Cipher Suite Used by your ASA

Use this procedure to identify the OpenSSL cipher suite being used by your ASA. If the cipher suite named in the command output is not in the Cipher Suites Supported by CDO's Secure Device Connector, the SDC doesn't support that cipher suite and you will need to update the cipher suites on your ASA.

Step 1 Open a console window on a computer that can reach the SDC.

Step 2 Connect to your SDC using SSH. You can log in as a regular user such as CDO or SDC or some other user you created. You don't need to be logged in as root.

Tip To find your SDC IP address:

a. Open CDO.

b. From the user menu, select Secure Device Connectors.

c. Click the SDC displayed in the table. The IP address of the SDC is displayed in the details pane for the device.

Step 3 At the command prompt enter: **openssl s_client -showcerts -connect** *ASA_IP_Address***:443**

Step 4 Look for these lines in the command output.

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

In this example, the cipher suite being used by the ASA is `DES-CB3-SHA`.

Cipher Suites Supported by CDO's Secure Device Connector

CDO's Secure Device Connector uses node.js which only accepts the latest and most secure ciphers. As a result, CDO's SDC only supports this list of ciphers:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

If the cipher suite you use on your ASA is not in this list, SDC does not support it and you will need to Updating your ASA's Cipher Suite.

Updating your ASA's Cipher Suite

To update the TLS cipher suites on an ASA:

Step 1 Connect to the ASA using SSH.

Step 2 Once connected to the ASA, elevate your privileges to global configuration mode. Your prompt should look like this: asaname(config)#

Step 3 At the prompt, enter a command similar to this:

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA256"
```

Note The cipher suites this command configures your ASA to support are contained between quotes and after the word custom. In this command, the cipher suites specified begin with `ECDHE-RSA-AES128-GCM-SHA256` and end with `DHE-RSA-AES256-SHA256`. When you enter the command on your ASA, remove any cipher suites you know your ASA will not support.

Step 4 After you submit the command, enter write memory at the prompt to save the local configuration. For example:

```
asaname(config)#write memory
```

Troubleshoot ASA using CLI commands

This section discusses some of the important commands you may want to use to troubleshoot the ASA and test basic connectivity. See CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide to learn about other troubleshooting scenarios and CLI commands. In the 'System Administration' section, navigate to the 'Testing and Troubleshooting' chapter.

You can use the CDO CLI interface available for each ASA device to execute these commands. See CDO Command Line Interface to learn about how to use the CLI interface in CDO.

NAT Policy Settings

Some of the important commands to determine the NAT settings are as follows:

- To determine NAT policy statistics, use **show nat**.

- To determine the NAT pools, including the addresses and ports allocated, and how many times they were allocated, use **show nat pool**.

For more commands related to NAT, see CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, and navigate to the 'Network Address Translation (NAT)' chapter.

Test Basic Connectivity: Pinging Addresses

You can ping the ASA device using the **ping <IP address>** command using the ASA CLI interface. To learn about

Display the Routing Table

Use the **show route** command to view the entries in the routing table.

ciscoasa# show route

Example output for a routing table of an ASA:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, + - replicated route

SI - Static InterVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management

C 10.0.0.0 255.0.0.0 is directly connected, Outside

L 10.10.10.1 255.255.255.255 is directly connected, Outside

C 192.168.0.0 255.255.255.0 is directly connected, management

L 192.168.0.118 255.255.255.255 is directly connected, management
```

Monitor Switch Ports

- **show interface**

  Displays interface statistics.

- **show interface ip brief**

  Displays interface IP addresses and status.

- **show arp**

Shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds.

Example output of ARP entries:

```
management 10.10.32.129 0050.568a.977b 0

management 10.10.32.136 0050.568a.5387 21

LANFAIL 20.20.21.1 0050.568a.4d70 96

outsi 10.10.16.6 0050.568a.e6d3 3881

outsi 10.10.16.1 0050.568a.977b 5551
```

Troubleshoot ASA Remote Access VPN

This section discusses some of the troubleshooting issues that may occur when configuring remote access VPN on an ASA device.

Missing Information on the RA VPN Monitoring Page

This issue may occur if the outside interface is not enabled for Webvpn.

Resolution:

1. Select the RA VPN headend ASA device that is having issues.
2. In the **Management** pane on the right, click **Configuration**.
3. Click **Edit** and search for 'webvpn'.
4. Press **Enter** and add `enable` *interface_name*. Here, the interface_name is the name of the outside 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.

   For example:

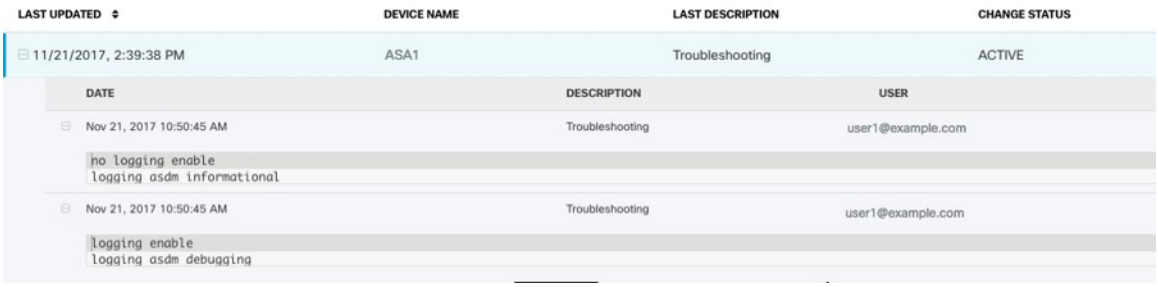
   ```
   webvpn

   enable outside
   ```

5. Click **Save**.
6. Preview and Deploy Configuration Changes for All Devices the configuration to the device.

ASA Real-time Logging

Use real-time logging to display the last 20 seconds of logged data or the last 10 KB of logged data, whichever limit is reached first. When CDO retrieves the real-time data, it reviews the existing logging configuration on your ASDM, changes it to request debugging-level data, and then returns the logging configuration to your configuration. The logging CDO displays reflects any logging filters you may have set in ASDM.

You can see the commands that CDO sends to perform logging by reviewing the change log. Below is an example of a change log entry. The first entry (on the bottom) indicates that CDO "turned on" logging with the logging enable command and changed the ASDM logging level to debugging. The second entry (on the top) shows that the logging configuration was returned to its previous state. Logging was "turned off" with the no logging enable command and the ASDM logging level was returned to informational.



View ASA Real-time Logs

Step 1 Click the appropriate device type tab and select the device for which you want to view real-time data.

Step 2 Click **Troubleshoot** Troubleshoot .

Step 3 (Optional) Before clicking View Real-time Log, you can define a filter in the left pane to refine the results of your logging search.

Step 4 Click **View Real-time Log**. CDO retrieves the real-time logging data based on your filterin criteria and displays it.

Step 5 To see an additional 20 seconds of logged data or the last 10 KB of logged data. click **View Real-Time Log** again.

ASA Packet Tracer

Packet tracer allows you to send a synthetic packet into the network and evaluate how the existing routing configuration, NAT rules, and policy configurations, affect that packet. Use this tool to troubleshoot these kinds of issues:

- Users report that they cannot reach resources that they should be able to.
- Users report that they can reach resources they should not be able to.
- Test a policy to determine if it works as you expect.

Packet tracer can be used on a live, online, ASA device either physical or virtual. Packet Tracer does not work on Device Types. Packet tracer evaluates packets based on the saved configuration on the ASA. Staged changes on CDO are not evaluated by packet tracer.

We consider it a best-practice to run packet tracer on an ASA that is in the synced state. Though packet tracer will run if the device is not synced, you could encounter some unexpected results. For example, if you deleted a rule in the staged configuration on CDO, and this same rule was triggered on the ASA during packet tracing, CDO won't be able to show you the result of the packet's interaction with that rule.

Troubleshooting with ASA Packet Tracer

As packet tracer sends the packet through the routing configuration, NAT rules, and security policies of your ASA, it displays the packet's status at each step. If the packet is allowed by the policy it receives a green checkmark . If a packet is denied and dropped, CDO displays a red X .

Packet tracer also displays a real time log of the result of the packet trace. In the example below, you can see where a rule denied a tcp packet.

Troubleshoot an ASA Device Security Policy

Step 1 In the pane, select the interface and packet type you want to send virtually through your ASA.

Step 2 (Optional) If you want to trace a packet where the security group tag value is embedded in the Layer 2 CMD header (Trustsec), check SGT number and enter the security group tag number, 0-65535.

Step 3 Specify the source and destination. You can specify IPv4 or IPv6 addresses, fully-qualified domain names (FQDN), or security group names or tags if you use Cisco Trustsec. For the source address, you can also specify a username in the format Domain\username.

Step 4 Specify other protocol characteristics:

- ICMP-Enter the ICMP type, ICMP code (0-255), and optionally, the ICMP identifier.
- TCP/UDP/SCTP-Enter the source and destination ports by selecting them from the list or entering a value in the port combo box.
- IP-Enter the protocol number, 0-255.

Step 5 Click **Run Packet Tracer**.

Step 6 Continue with Analyze Packet Tracer Results.

Troubleshoot an Access Rule

Step 1 Select a policy that is associated with your ASA.

Step 2 Select a rule in the network policy to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. Notice that in the values panel of the troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.

Step 3 Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer button becomes active.

Step 4 Click **Run Packet Tracer.**

Step 5 Continue with Analyze Packet Tracer Results.

Troubleshoot a NAT Rule

Step 1 Select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.

Step 2 Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. Notice that in the values panel of the Troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.

Step 3 Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.

Step 4 Click **Run Packet Tracer.**

Step 5 Continue with Analyze Packet Tracer Results.

Troubleshoot a Twice NAT Rule

Step 1 Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. For a bi-directional Twice NAT rule, this opens a dropdown where you choose to troubleshoot the source packet translation or the destination packet translation.

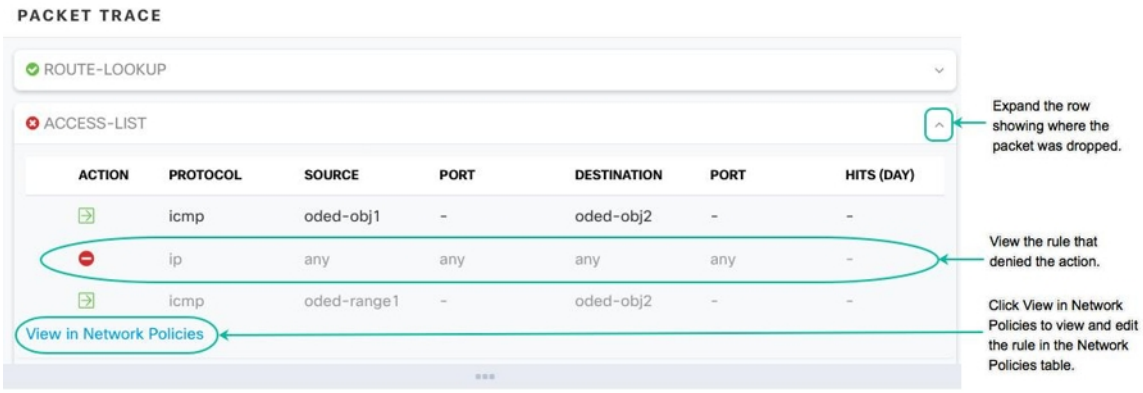
Step 2 Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.

Step 3 Click **Run Packet Tracer**.

Analyze Packet Tracer Results

Whether the packet is dropped or allowed, you can learn why by expanding a row in the packet trace table and reading the rule or logging information related to that action. In the example below, packet tracer identified an access list policy that included a rule to deny an IP packet coming from any source and going to any destination. If this is not the action you want, you can click the **View in Network Policies** link and edit that rule immediately. After you edit the rule, be sure to deploy that configuration change to the ASA and then re-run packet tracer to ensure that you get the access results you expect.

Along with the packet tracer results, CDO displays the ASA Real-time Logging from the ASA.



Cisco ASA Advisory cisco-sa-20180129-asa1

The Cisco Product Security Incident Response Team (PSIRT) **published the security advisory** cisco-sa-20180129-asa1 which describes a critical-severity ASA and Firepower security vulnerability. Read the entire PSIRT team advisory for a full explanation of what ASA and Firepower hardware, software, and configurations are affected.

If you determine that your ASAs are impacted by the advisory, you can upgrade your ASAs to the patched version using CDO. Use this process:

Step 1 Configure DNS on ASA on each ASA that is affected.

Step 2 Return to the advisory to determine which software patch you need.

Step 3 See Upgrade ASA and ASDM Images on a Single ASA, on page 138 for topics that describe how to use CDO to upgrade your ASAs to the fixed releases listed in the ASA advisory. Start with the Prerequisites for ASA and ASDM Upgrade in CDO and then read about upgrading individual ASAs, upgrading ASAs in an active-standby configuration, or upgrading ASAs in bulk.

For your convenience, here is the summary of the security advisory that Cisco reported:

UPDATED 2/5/2018: After further investigation, Cisco has identified additional attack vectors and features that are affected by this vulnerability. In addition, it was also found that the original fix was incomplete so new fixed code versions are now available. Please see the Fixed Software section for more information. A vulnerability in the XML parser of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. It was also possible that the ASA could stop processing incoming Virtual Private Network (VPN) authentication requests due to a low memory condition. The vulnerability is due to an issue with allocating and freeing memory when processing a malicious XML payload. An attacker could exploit this vulnerability by sending a crafted XML packet to a vulnerable interface on an affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, cause a reload of the affected device or stop processing of incoming VPN authentication requests. To be vulnerable the ASA must have Secure Socket Layer (SSL) services or IKEv2 Remote Access VPN services enabled on an interface. The risk of the vulnerability being exploited also depends on the accessibility of the interface to the attacker. For a comprehensive list of vulnerable ASA features please refer to the table in the Vulnerable Products section. Cisco has released software updates that address this vulnerability. There are no workarounds that address all the features that are affected by this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

Confirming ASA Running Configuration Size

To confirm the size of your running configuration file, follow this procedure:

Step 1 Access the ASA's command line interface in one of these ways:

- Open a terminal window and log into your ASA using SSH. Elevate your privilege to "privileged EXEC" mode so you see the prompt with `hostname#` .
- If you managed to get your ASA onboarded, open the **Inventory** page, select the device you want to connect to, and click **>_ Command Line Interface** button in the Device Actions pane.

Step 2 At the prompt type `copy running-config flash`

Step 3 When prompted for the Source filename, don't type anything and press <Enter>

Step 4 When prompted for the destination filename, enter a name for the output file. After ASA copies the running configuration the file you specified, it returns you to the privileged EXEC prompt.

Step 5 At the prompt, type `show flash`

Step 6 Look in the length column. If your file is over 4718592 bytes, it is larger than 4.5 MB.

Here is a sample set of commands and output:

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

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 CDO customers:

- Customers using CDO's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the CDO 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 CDO-Standard SDC Host

Use these instructions if you Deploy a Secure Device Connector Using CDO's VM Image

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 CDO 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

Large ASA Running Configuration Files

Behavior in CDO

You may see behavior such as the ASA failing to onboard, CDO not displaying all of the configuration defined in the ASA's running configuration file, or CDO failing to write to the change log.

Possible Cause

The running configuration file of your ASA may be "too large" for CDO.

When you an onboard an ASA to CDO, CDO stores a copy of the ASA's running configuration file in its database. Generally, if that running configuration file is too large (4.5 MB or larger), or it contains too many lines (approximately 22,000 lines), or there are too many access-list entries for a single access group, CDO will not be able to predictably manage that device.

To confirm the size of your running configuration file, see Confirming ASA Running Configuration Size.

Workaround or Solution

Contact your Cisco account team for help safely reducing the size of your configuration file without disrupting your security policies.

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 CDO 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 CDO in a row. If your SDC is unreachable, your tenant will not be able to communicate with any of the devices you have onboarded.

CDO 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 CDO 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 CDO IP address in your region. See Connect CDO to your Managed Devices, on page 9.
2. Attempt to reconnect CDO 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 CDO after Deployment, on page 478.

.

SDC Status not Active on CDO after Deployment

If CDO does not indicate that your SDC is active in about 10 minutes after deployment, connect to the SDC VM using SSH using the `cdo` user and password you created when you deployed the SDC.

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`, CDO still does not indicate that the SDC is **Active**, Contact CDO Support.

Changed IP Address of the SDC is not Reflected in CDO

If you changed the IP address of the SDC, it will not be reflected in CDO until after 3:00 AM GMT.

Troubleshoot Device Connectivity with the SDC

Use this tool to test connectivity from CDO, 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 CDO can reach your device.

Step 1 Select the SDC.

Step 2 In the **Troubleshooting** pane on the right, click **Device Connectivity**.

Step 3 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**. CDO 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, CDO 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 4 If you continue to have issues onboarding or connecting to the device, Contact CDO 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 in the **Services** page from CDO 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 CDO customers:

- Customers using CDO's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the CDO 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 CDO-Standard SDC Host, on page 476
  - Updating a Custom SDC Host, on page 477
  - Bug Tracking, on page 477

Updating a CDO-Standard SDC Host

Use these instructions if you Deploy a Secure Device Connector Using CDO's VM Image

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 CDO 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

Cisco Defense Orchestrator is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, CDO 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, CDO will no longer be able to communicate with your devices through the SDC.

CDO'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.

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 CDO 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 CDO operations team can complete your SDC migration to the new communication method.

SDC version is lower than 202311****

Cisco Defense Orchestrator (CDO) is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, CDO 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, CDO will no longer be able to communicate with your devices through the SDC.

CDO'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 CDO 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, CDO operations will be able to run the migration process again.

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`. CDO 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 CDO.
b) Navigate to the Secure Connectors page by navigating from the CDO 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 CDO operations team can run the migration process again.

Certificate or Connection errors with AWS servers

CDO is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, CDO 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, CDO will no longer be able to communicate with your devices through the SDC.

CDO'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.

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 CDO operations team can complete your SDC migration to the new communication method.

Secure Event Connector Troubleshooting

If none of these scenarios match yours, How CDO 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 28. 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 371.

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 CDO 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/CDO/es_bootstrapdata") does not exist, exiting.

Diagnosis: SEC Bootstrap data file("/usr/local/CDO/es_bootstrapdata") is not present.

Repair: Place the SEC bootstrap data generated in CDO UI onto the file **/usr/local/**CDO**/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 CDO UI onto the file **/usr/local/**CDO**/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/CDO/data/<tenantDir>/event_streamer/logs/startup.log).
3. If so, run SEC Cleanup Command and try onboarding again.

Contact CDO Support

If none of these scenarios match yours, How CDO 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:

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.

Step 1 Click the **Historical** tab.

Step 2 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 3 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 4 Enter the user's IP address in the **Source IP** field in the Events filter bar.

Step 5 If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.

Step 6 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 7 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 Configuring NSEL for ASA Devices by Using a CDO Macro , 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 490.
2. Uncompress the sec_troubleshoot.tar.gz file, on page 491.

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:

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 CDO 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 491.

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:

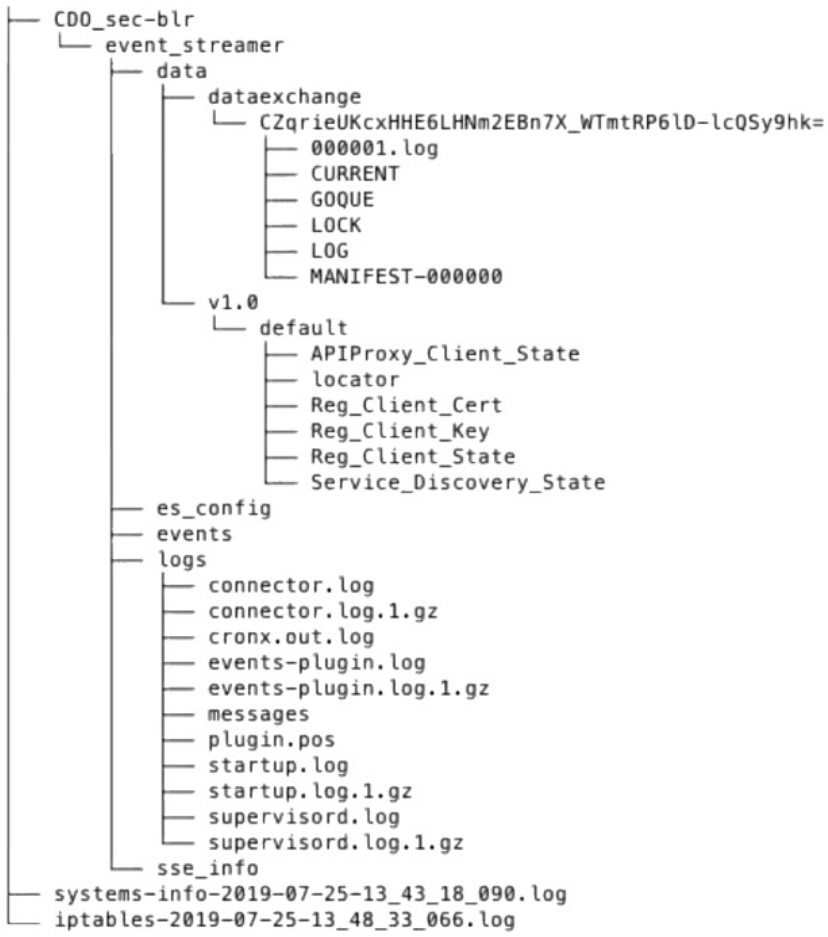
   ```
   [cdo@localhost ~]$sudo su root
   ```

   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 CDO, 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 CDO Customers Open a Support Ticket with TAC.

SEC Status is Inactive in CDO

Symptom: The Secure Event Connector status shows "Inactive" in the CDO 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 CDO Event Logging Page

Symptom: The Secure Event Connector shows "Active" in CDO Secure Connectors page but you do not see events in CDO Event viewer.

Solution or workaround:

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/CDO/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/CDO/data/<tenantDir>/event_streamer/logs/events-plugin.log) and ensure that the events are being processed. If not, How CDO 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 CDO Customers Open a Support Ticket with TAC.

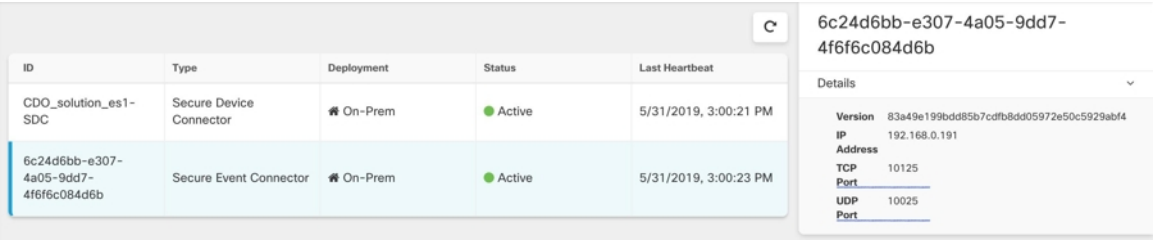
estreamer-connector RUNNING pid 36, uptime 5:25:17

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 CDO 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 488 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 CDO and click **Settings**. Scroll down the page to locate your **Tenant Name**.

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 494

SEC Cleanup Command Failure

Use this procedure if the SEC Cleanup Command, on page 494 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:

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:

Step 1 Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).

Step 2 Login to the SDC as "CDO" user.

Step 3 Switch to the "sdc" user:

```
[cdo@tenant]$sudo su sdc
```

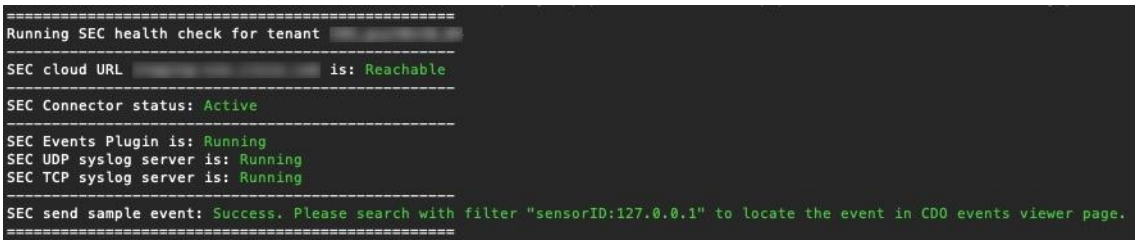
Step 4 At the prompt, run the healthcheck.sh script and specify the tenant name:

```
[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:



Values of Health Check output:

- **SEC Cloud URL**: Displays the CDO cloud URL and whether or not the SEC can reach CDO.
- **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 CDO.
- **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 Cisco Defense Orchestrator

Troubleshooting Login Failures

Login Fails Because You are Inadvertently Logging in to the Wrong CDO Region

Make sure you are logging into the appropriate CDO 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 CDO in Different Regions, on page 4 for information about which region you shoud sign into.

Troubleshooting Login Failures after Migration

Login to CDO Fails Because of Incorrect Username or Password

Solution If you try to log in to CDO 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 67.

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

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your CDO tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between CDO 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 CDO tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Defense Orchestrator APJ
  - **Solution** Cisco Defense Orchestrator Australia
  - **Solution** Cisco Defense Orchestrator EU
  - **Solution** Cisco Defense Orchestrator India
  - **Solution** Cisco Defense Orchestrator US
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Access and Certificates

Troubleshoot User Access with CDO

Consider the case of users being denied access to a resource that they should have access to. Here is an approach you can take to diagnose and remediate that problem.

Step 1 Users inform your security team that their access to a resource is blocked. Determine how that resource is typically reached. What is it's IP address? Do you reach it on a specific port? What protocol is used to send information to the resource?

Step 2 From the **Inventory** page, click the **Devices** tab.

Step 3 Click the **FTD** tab and select the ASA and run packet tracer. See ASA Packet Tracer for more instructions.

Step 4 Examine the packet trace table for rules that may have denied access to the resource.

Step 5 After identifying the rule denying access, create a change request label in CDO and enable it. See Change Request Management, on page 326. This will help you identify in Change Log policy changes you made to allow access to the resource.

Step 6 Edit the rule from CDO to correct the behavior. Your ASA is now out of sync with CDO.

Step 7 Deploy the changes to the ASA from the **Inventory** page. CDO traces packets through the configuration saved on the ASA not a configuration staged on CDO. Be aware, you will also be deploying any other configuration changes staged on CDO to your ASA.

Step 8 Re-run packet tracer to determine if the policy change provides the desired results. Confirm that your users now have access to the resource.

Step 9 Assuming your users now have access, clear the change request label in CDO. This prevents unrelated activity from being associated with this fix.

Note If the change you made doesn't fix the problem or creates some new problems and you want to return to your previous configuration, you can do restore the ASA Configuration. See Restore an ASA Configuration.

Resolve New Fingerprint Detected State

Step 1 In the navigation bar, click **Inventory**.

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 CDO 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.

Step 1 Click the **Historical** tab.

Step 2 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 3 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 4 Enter the user's IP address in the **Source IP** field in the Events filter bar.

Step 5 If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.

Step 6 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 7 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.`

Troubleshooting Login Failures after Migration

Login to CDO Fails Because of Incorrect Username or Password

Solution If you try to log in to CDO 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 67.

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

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your CDO tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between CDO 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 CDO tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Defense Orchestrator APJ
  - **Solution** Cisco Defense Orchestrator Australia
  - **Solution** Cisco Defense Orchestrator EU
  - **Solution** Cisco Defense Orchestrator India
  - **Solution** Cisco Defense Orchestrator US
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Objects

Resolve Duplicate Object Issues

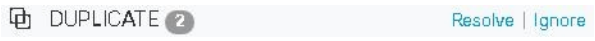
Duplicate objects are two or more objects on the same device with different names but the same values. These objects are usually created accidentally, serve similar purposes, and are used by different policies. After resolving duplicate object issues, CDO updates all affected object references with the retained object name.

To resolve duplicate object issues:

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**. CDO 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. CDO 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 CDO shows you.
- Click **Ignore All** if you want to keep the object but do not want CDO 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.

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 82
- Bulk Reconnect Devices to CDO, on page 86

Resolve an Unused Object Issue

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 CDO.
- In the Issues pane, click **Ignore.** If you ignore an object, CDO 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 233 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

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.

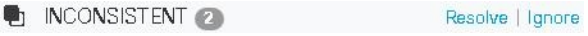
Step 4 In the Actions pane on the right, click **Remove** to remove all the unused objects you selected in CDO. You can remove 99 objects at a time.

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:** CDO ignores the inconsistency between objects and retains their values. The objects will no longer be listed under the inconsistency category.
- **Merge:** CDO combines all selected objects and their values into a single object group.
- **Rename:** CDO allows you to rename one of the inconsistent objects and give it a new name.
- **Convert Shared Network Objects to Overrides:** CDO 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:** - CDO 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, CDO 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 CDO.

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:

Step 1 In the CDO 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**. CDO 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 502 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.

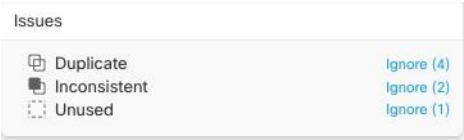
Important If the object becomes associated with another issue type at a later time, the ignore action you committed only affects the issues you selected at that time. For example, if you ignored an object because it was a duplicate and the object is later marked inconsistent, ignoring it as a duplicate object does not mean it will be ignored as an inconsistent object.

To ignore issues in bulk, follow this procedure:

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 CDO 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 CDO. 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, CDO 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 CDO.	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 505
Invalid credentials	Username and password combination used by CDO to connect to the device is incorrect.	Troubleshoot Invalid Credentials, on page 506
Onboarding	Device onboarding is initiated but is not complete.	Check you device's connectivity and ensure you complete the device registration.
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 506
Onboarding Error	CDO may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error, on page 514

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 CDO portal by signing out from CDO 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:

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 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 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:

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

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**. CDO 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 CDO attempted to use the wrong credentials to connect to the device, the username and password combination CDO 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 CDO and the device.

Troubleshoot New Certificate Issues

CDO's Use of Certificates

CDO checks the validity of certificates when connecting to devices. Specifically, CDO 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 CDO uses certificates differently than browsers:

- In the case of self-signed certificates, CDO overrides the domain name check, instead checking that the certificate exactly matches the one trusted by an authorized user during device onboarding or reconnection.

- CDO 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 CDO, 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, CDO 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 CDO with an invalid certificate.

Identifying Certificate Issues

There are several reasons that CDO may not be able to onboard a device. When the UI shows a message that "CDO 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 CDO 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, CDO 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 CDO. 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 CDO more than one managed device to CDO at the same time, CDO 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. Navigate to the **Inventory** page.
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**. CDO 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**.

   CDO automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the **Inventory** page to see the device once it's synched.

Certificate Error Codes

Verify return code: 0 (ok) but CDO returns certificate error

Once CDO 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, CDO 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 CDO 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, CDO 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 CDO. 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 CDO more than one managed device to CDO at the same time, CDO 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:

Step 1 In the navigation bar, click **Inventory**.

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**. CDO 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**.

CDO automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the **Inventory** page to see the device once it's synched.

Troubleshoot Onboarding Error

The device onboarding error can occur for various reasons.

You can take the following actions:

Step 1 On the **Inventory** page, click the **Devices** tab.

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 CDO and try onboarding the device again.

Resolve the Conflict Detected Status

CDO allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 243 is enabled and there was a change made to the device's configuration without using CDO, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Conflict Detected** state and continue from Step 4.

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 CDO.
- 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** CDO with the device's running configuration.

  Note As CDO 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 CDO.

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:

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

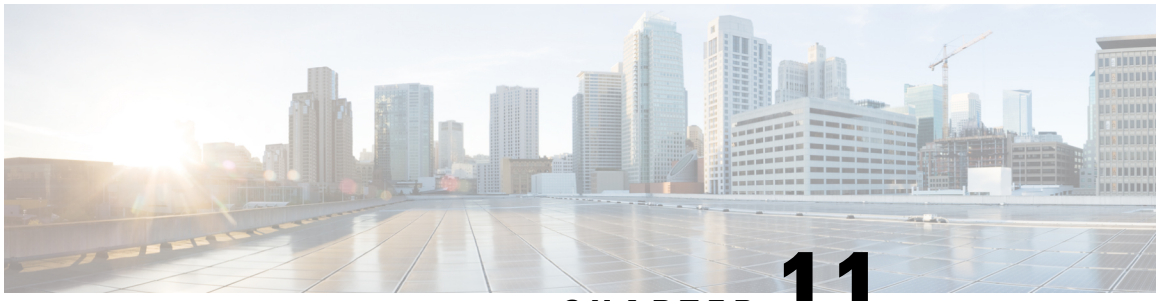
Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

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 CDO 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 CDO to the device, or you want to "undo" the configuration changes you started making on CDO. This option overwrites the configuration stored in CDO with the running configuration stored on the device.



CHAPTER 11

FAQ and Support

This chapter contains the following sections:

Cisco Defense Orchestrator

What is Cisco Defense Orchestrator?

Cisco Defense Orchestrator (CDO) 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 CDO 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

CDO administrators can monitor and maintain all these device types through a single interface.

FAQ About Onboarding Devices to Cisco Defense Orchestrator

FAQs About Onboarding Secure Firewall ASA to CDO

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 CDO 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 Defense Orchestrator to get started.

FAQs About Onboarding FDM-Managed Devices to CDO

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 CDO. Onboarding an On-Prem Management Center also onboards all of the devices registered to the On-Prem Management Center. CDO 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 CDO

How do I onboard a Meraki device?

MX devices can be managed by both CDO and the Meraki dashboard. CDO 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 CDO

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 inventory page.

FAQs About Onboarding IOS Devices to CDO

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 Inventory 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 CDO. You can use an ASA model to analyze the configuration of an ASA device without onboarding the device itself.

When is a device Synced?

When the configuration on CDO and the configuration stored locally on the device are the same.

When is a device Not Synced?

When the configuration stored in CDO 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 CDO (out-of-band), and is now different than the configuration stored on CDO.

What is an out-of-band change?

When a change is made to the device outside of CDO. 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 CDO 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 CDO, CDO maintains a copy of its configuration. When you make a change on CDO, CDO makes a change to its copy of the device's configuration. When you "deploy" that change back to a device, CDO 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 233
- Deploy Configuration Changes from CDO to ASA

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?

CDO's cloud architecture allows it to scale to thousands of devices.

Does CDO manage Cisco Integrated Services Routers and Aggregation Services Routers?

CDO 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 CDO manage SMA?

No, CDO does not currently manage SMA.

Security

Is CDO Secure?

CDO offers end-to-end security for customer data through the following features:

- Initial Login to Your New CDO Tenant, on page 3
- Authentication calls for APIs and database operations
- Data isolation in flight and at rest
- Separation of roles

CDO 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 CDO is encrypted with SSL, and all customer-tenant data volumes are encrypted.

CDO's multi-tenant architecture isolates tenant data and encrypts traffic between databases and application servers. When users authenticate to gain access to CDO, 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.

CDO 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 CDO 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 Cisco Defense Orchestrator cloud platform?

Yes. The secured connection is performed using the CDO SDC which is used as a proxy between the device and CDO platform. CDO 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 CDO 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

CDO 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 CDO 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 CDO 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 CDO 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 CDO; directly to a device), comparing the configuration present in CDO that of the device, CDO presents additional metadata that were not added or modified by me. Why?

As CDO 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 CDO 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 CDO. A device is "claimed" if its serial number has been onboarded to a CDO tenant.
- **Parked** - Used in the context of serial number onboarding in CDO. A device is "parked" if it has connected to the Cisco Cloud, and a CDO 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 CDO tenant if its serial number has already been "claimed," or the FTD is "parked" in the Cisco cloud until a CDO 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?

Cisco Defense Orchestrator 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. For more information, see Manage ASA Network Security Policy.

Note CDO supports only fully shadowed rules.

Connectivity

The Secure Device Connector changed IP address, but this was not reflected within CDO. What can I do to reflect the change?

In order to obtain and update the new Secure Device Connector (SDC) within CDO, 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 CDO 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 CDO uses to connect to the device (see Changing a Device's IP Address in CDO, on page 81) and then reconnect the device (see Bulk Reconnect Devices to CDO, on page 86). 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 CDO?

- 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.

About Data Interfaces

You can use either the dedicated management interface or a regular data interface for communication with the device. CDO 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. CDO 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 CDO. 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 CDO Processes Personal Information

To learn how Cisco Defense Orchestrator processes your personal identifiable information, see the Cisco Defense Orchestrator Privacy Data Sheet.

Contact CDO 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:

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 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 CDO account can open a support ticket with Cisco's Technical Assistance Center (TAC).

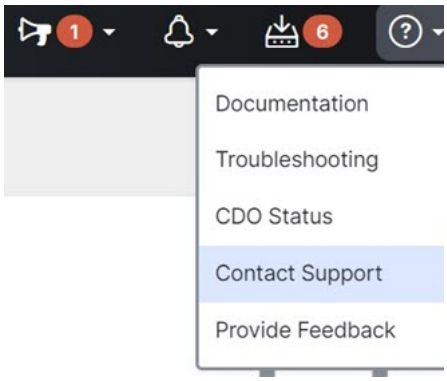
- How CDO Customers Open a Support Ticket with TAC.
- How CDO Trial Customers Open a Support Ticket with TAC.

How CDO Customers Open a Support Ticket with TAC

This section explains how a customer using a licensed CDO tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Step 1 Log in to CDO.

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 Defense Orchestrator 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.

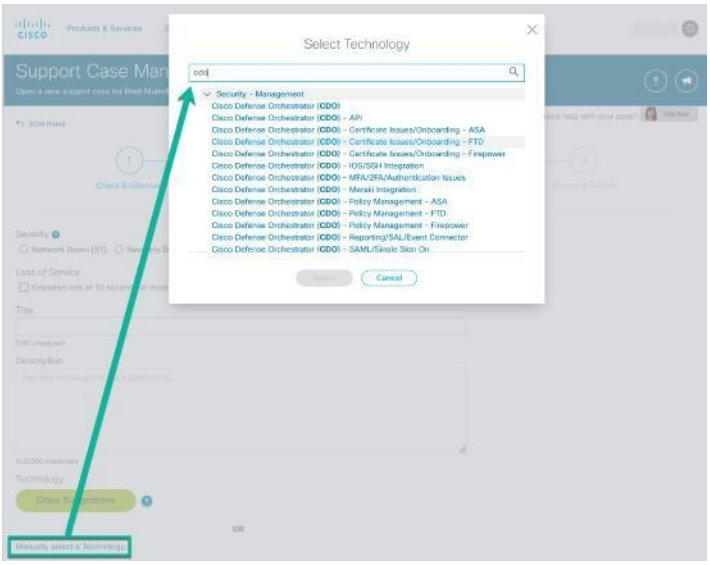
- **Important**: In order for your case to be associated with your Cisco.com account, you need to associate your contract number to your Cisco.com profile. Use this procedure to associate your contract number to your Cisco.com profile.
  a. Open to Cisco Profile Manager.
  b. Click the **Access Management** 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 **CDO** in the search field.

Step 12 Select the category that best matches your request, and click **Select**.



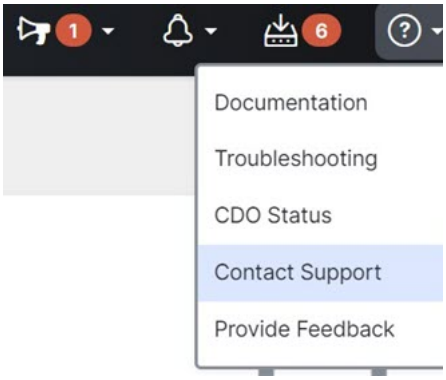
Step 13 Complete the remainder of the service request and click **Submit**.

How CDO Trial Customers Open a Support Ticket with TAC

This section explains how a customer using a free trial of a CDO tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Step 1 Log in to CDO.

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.

CDO Service Status Page

CDO maintains a customer-facing service status page that shows you if the CDO 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 CDO status page by clicking **CDO Status** in the help menu on any page in CDO.

On the status page, you can click the **Subscribe to Updates** to receive a notification if the CDO service goes down.