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 for your Super Admin 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 or Deploy a Secure Device Connector On Your VM 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.

Managing ASA with Cisco Defense Orchestrator

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 bulk or one at a time. See 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 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 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 unused objects. 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 objects. 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.

Managing ASA with Cisco Defense Orchestrator

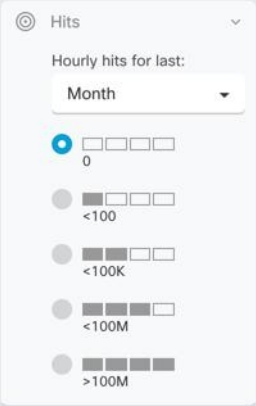
3. Resolve inconsistent objects. Inconsistent objects are objects with the same name, but different values, on two or more devices. Sometimes users create objects in different configurations with the same name and content, but over time the values of these objects diverge, which creates the inconsistency. 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 shadow 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.

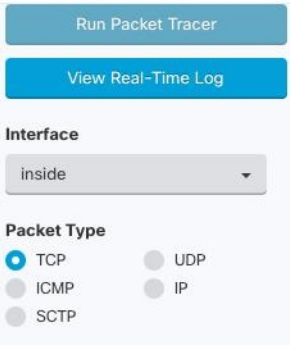
Evaluate Policy Hit Rates

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

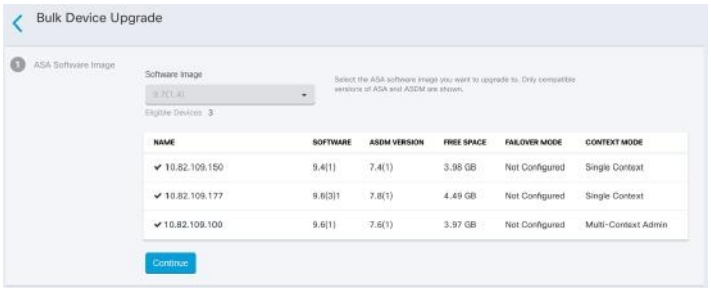
You can use the ASA Packet Tracer to test the path of a synthetic packet through a policy and determine if a rule is inadvertently blocking or allowing access.



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.

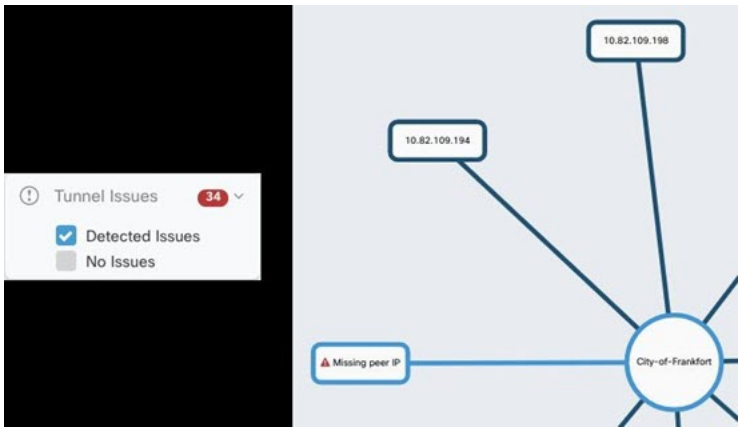
CDO periodically reviews its database and adds the newest ASA and ASDM images to it. CDO only supports generally available (GA) images and does not add custom images to its database. If you do not see a specific GA image in the list, please contact Cisco TAC from the **Contact Support** page. We will 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 and then continue with Upgrade Multiple ASAs with Images from your own Repository 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.



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 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 for more information.

Monitor Device Configuration Synchronization

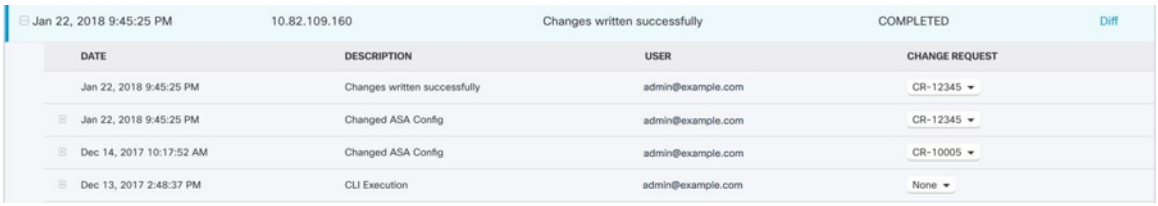
CDO periodically compares the device configuration it has stored in its database with the one installed on the ASA. The ASA you onboarded to CDO can still be onboarded ASA can still be managed by the device's Adaptive Security Device Manager (ASDM), so CDO makes sure that the configuration it has is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

Managing ASA with Cisco Defense Orchestrator



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 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 command line interface (CLI) to manage your devices one at a time or many at once.

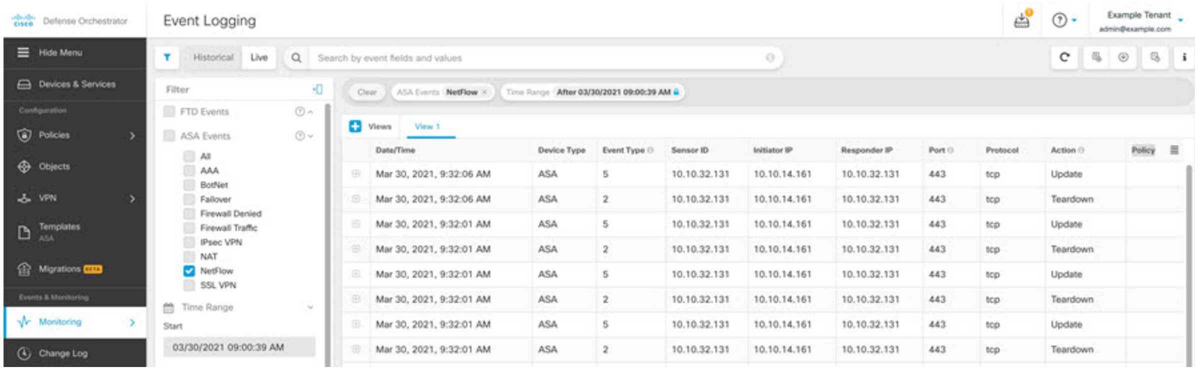
ASA CLI users will appreciate the extra capabilities of our CLI tool. Here are some of the reasons to use CDO's CLI tool rather than connecting to the device with an SSH session:

- 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 allows you to direct syslog events and Netflow Secure Event Logging (NSEL) events from your ASA to a Secure Event Connectors (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.

Managing ASA with Cisco Defense Orchestrator



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.

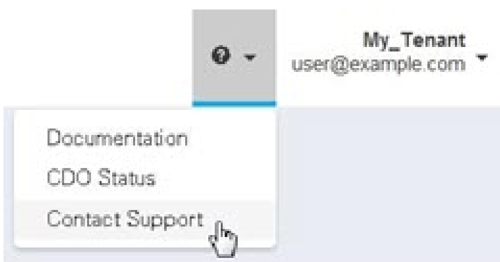
See Implementing Secure Logging Analytics (SaaS) for ASA Devices for a complete explanation of how to implement Cisco Security Analytics and Logging.

What to do Next

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

If You Need Help

You can contact support, ask a question, or read our product documentation by clicking on our support menu in the CDO GUI.



Managing ASA with Cisco Defense Orchestrator