Managing On-Prem FMC with Cisco Defense Orchestrator

First Published: 2021-02-12

Last Modified: 2024-04-24

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2024 Cisco Systems, Inc. All rights reserved.

Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator

• Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator, on page iii

Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator

About On-Prem Firewall Management Center

On-Prem Management Center support is limited to onboarding, viewing its managed devices, viewing, managing network objects and cross-launching to On-Prem Management Center UI to manage associated devices and objects. Additional features will be supported soon. For functionality that may not be supported by CDO at this time, you must use the On-Prem Management Center console. See the Cisco Secure Firewall Management Center Configuration Guide of the version your system is running, to know more about the features provided by On-Prem Management Center.

The On-Prem Management Center is a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks. It is a management console that is comparable, but not identical, to ASDM and FDM. For a list of On-Prem Management Center devices and software versions that CDO supports, see Devices, Software, and Hardware Supported by CDO.

Version Support

CDO supports version 6.4 and later. An On-Prem Management Center can manage older devices, usually a few major versions back. For example, devices running version 6.6.0 can manage a Version 6.4.0 device. If an On-Prem Management Center manages a device that is running a version earlier than 6.4, the device may be displayed in the **Inventory** page, but cannot be deployed to or its policies modified from CDO. You must make changes and deploy from the On-Prem Management Center UI.

Note If a managed device is disabled, or unreachable, CDO may display the device in the **Inventory** page, but cannot successfully send requests or view device information.

How does CDO Communicate with an FMC

CDO acts as a REST API client to send requests to the On-Prem Management Center, and the On-Prem Management Center then uses its designated client to channel the requests to its managed devices. Because the device does not allow multiple logins with the same login credentials, we recommend creating a new user on the On-Prem Management Center specifically for CDO communication that has administrator-level permissions. This new user will have to be replicated on CDO, as either a CDO-provided Administrator or a custom user role with **system** and **devices** permission. Without an admin login, CDO will not be able to successfully use REST API commands to modify or create policy, rules, or objects.

Onboard or Remove an On-Prem Management Center

You can onboard or remove an On-Prem Management Center at any time. The On-Prem Management Center and its registered device must be running at least Version 6.4 to be read by CDO. To onboard an On-Prem Management Center and its registered devices, see Onboard an On-Prem Firewall Management Center to CDO with Credentials.

Once an On-Prem Management Center is onboarded, selecting the On-Prem Management Center from the **Services** page, clicking **Devices** under **Management** or any actions on the right pane opens up the **Verify FMC Cross Launch URL** wizard, which lets you enter the public IP address or the FQDN and the port number of your management center. Clicking **Continue** cross-launches to the selected On-Prem Management Center web UI in a new tab using the IP address you entered. You can also add external links manually in the **Add External Links** option under **External Links** on the right pane.

Removing an On-Prem Management Center from your CDO tenant also removes the devices registered to that On-Prem Management Center. See Remove an On-Prem Firewall Management Center from CDO for more information. If an On-Prem Management Center experiences an "Invalid Credentials" status after onboarding, you can **reconnect** the appliance. See Troubleshoot Invalid Credentials for more information.

Note Devices running Firepower 6.6 do not support the **reconnect** feature. If you have to reconnect the appliance, we recommend removing the On-Prem Management Center and re-onboarding the appliance.

On-Prem Management Center High Availability Pairs

CDO does not support high availability (HA) functionality for On-Prem Management Center appliances. If a pair of On-Prem Management Center appliances are configured for HA, the pair is listed as individual appliances in the **Services** page.

Devices Managed by an On-Prem Management Center

Once you onboard an On-Prem Management Center to CDO, all of the devices registered to that On-Prem Management Center are also read into CDO. From the **Inventory** page, you can see device information such as name, IP address, type of device, software version, and the state. Note that your On-Prem Management Center is displayed on the **Services** page and the devices it manages are listed on the **Inventory** page. In the **Services** page, you can see information such as version, devices managed, type of device, and status. Clicking the devices icon on the **Services** page, which displays the number of devices your FMC manages, takes you to the **Inventory** page, with the device filter applied, so all the devices managed by the On-Prem Management Center you selected are displayed.

You can perform actions using relevant options in the **Device Actions**, **Monitoring**, **Device Management**, and **Policies** panels on the right pane in the **Inventory**. If you select a device that is currently managed by an FMC and click these options, CDO automatically launches the On-Prem Management Center console that

manages the devices using the cross-launch URL you had entered. Use the filter icon to further organize the **Inventory** page. From here you can opt to view all the devices managed by the onboarded On-Prem Management Center, as well as the other supported device types. In addition, you can expand or collapse devices in a cluster and select them indivdually or as a group to perform actions.

Device Health Status

CDO displays the health status of threat defense devices in the **Inventory** page, such as **Normal**, **Error**, **Warning**, and **Disabled**; you can click the status of a device to navigate to the **Health Monitoring** page that corresponds to the device in the On-Prem Management Center user interface.

Note CDO keeps automatically updating the device health status every 10 minutes; however, you can do this manually by selecting the device and clicking **Check for Changes**.

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.

Objects

After you onboard an On-Prem Management Center to CDO, you can choose to discover objects from the On-Prem Management Center and manage them in CDO. You can do this by navigating to **Tools & Services** > **Firewall Management Center**, selecting the desired On-Prem Management Center, and clicking **Settings**. You can turn the **Discover & Manage Network Objects** toggle button on; when this option is enabled, CDO automatically reads all the objects from the On-Prem Management Center-managed devices into CDO. Once imported, the objects can be managed from CDO. Note that you need to have the super admin or admin user role to be able to use the **Settings** button.

When making a configuration change to an object from CDO, the change gets staged in CDO and you can manually push the change to the On-Prem Management Center after reviewing it from **Pending Changes**. In addition, when you make a configuration change to an object from the On-Prem Management Center user interface, CDO detects those changes as out-of-band changes that can be synchronized later. If you want your changes to be automatically synchronized with on-prem management center and not staged for review, turn the **Enable automatic sync of network objects** toggle on.

If you have existing objects in CDO that you want to assign to your On-Prem Management Center, select the On-Prem Management Center from the **Services** page and choose **Assign Objects** on the right pane. CDO displays all the existing objects and lets you select ones that you want to associate with the On-Prem Management Center that you selected. This heps promote consistency in network object definitions across platforms managed by CDO. Note that you can use the **Assign Objects** button only if **Discover & Manage Network Objects** is enabled for the selected on-prem management center.

Note

- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-prem management center that you have selected has one or more child domains or has the Chanage Management workflow enabled on it..
- You cannot turn the **Enable automatic sync of network objects** toggle on if the **Discover & Manage Network Objects** toggle is turned off.

On-Prem Management Center supports the following object types:

- Network Objects
- Network-Group Objects

Object Issues

CDO identifies the duplicate, inconsistent, or ununsed objects. You can filter the issues based on their issue states. However, CDO cannot resolve object issues.

Eventing

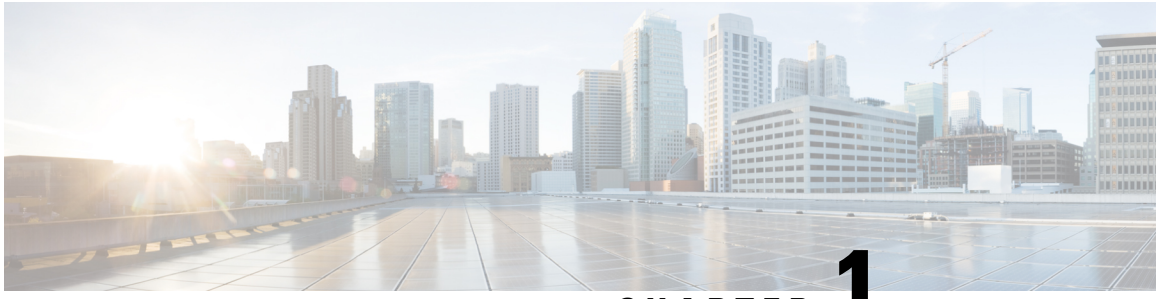
Searching and filtering the Historical and Live event tables for specific events, works the same way as it does when searching and filtering for other information in CDO. For more information, see Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your 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. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Firewall Analytics and Monitoring** package, the system can apply Secure Cloud Analytics dynamic entity modeling to your 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 device 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.



CHAPTER 1

Basics of Cisco Defense Orchestrator

Cisco Defense Orchestrator (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, on page 1
- Sign in to CDO, on page 2
- Migrate to **Cisco Security Cloud Sign On** Identity Provider, on page 4
- Launch a CDO Tenant, on page 5
- Manage Super Admins on Your Tenant, on page 6
- About CDO Licenses, on page 6
- Secure Device Connector, on page 8
- Devices, Software, and Hardware Supported by CDO, on page 36
- Browsers Supported in CDO, on page 38
- **CDO Platform Maintenance Schedule**, on page 38
- Manage a CDO Tenant, on page 39
- Manage Users in CDO, on page 53
- Active Directory Groups in User Management, on page 54
- Create a New CDO User, on page 58
- User Roles in CDO, on page 62
- Add a User Account to CDO, on page 66
- Edit a User Record for a User Role, on page 68
- Delete a User Record for a User Role, on page 68
- CDO Services Page, on page 69
- CDO Device and Service Management, on page 72
- CDO Inventory Information, on page 79
- CDO Labels and Filtering, on page 79
- Use CDO Search Functionality, on page 81
- Objects, on page 84

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 Cisco Defense Orchestrator 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 59. It is a four-step process. You need to complete all four steps.

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. Click the **CDO** tile to access defenseorchestrator.com or **CDO (EU)** to access defenseorchestrator.eu.

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 59.

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 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 account, click the CDO tile on the dashboard that corresponds to Cisco Defense Orchestrator(US), Cisco Defense Orchestrator (EU), or Cisco Defense Orchestrator (APJC)
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Launch a CDO Tenant

Step 1 Click the appropriate CDO button on the Cisco Security Cloud Sign On dashboard. The CDO tile directs you to https://defenseorchestrator.com, 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, on page 49 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 high availability pair, purchasing one 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 Cisco Defense Orchestrator 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 10 and Deploy a Secure Device Connector on your own VM, on page 13

Related Information:

- Connect Cisco Defense Orchestrator to your Managed Devices
- Update your Secure Device Connector, on page 26
- Remove a Secure Device Connector, on page 24

Connect Cisco Defense Orchestrator to your Managed Devices

CDO connects to the devices 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:

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 APJC region.

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 **United States** 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

If you are a customer in the **Asia-Pacific-Japan-China (APJC)** 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

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.

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 26 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 own VM, on page 13.

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 Cisco Defense Orchestrator 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.
- 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.

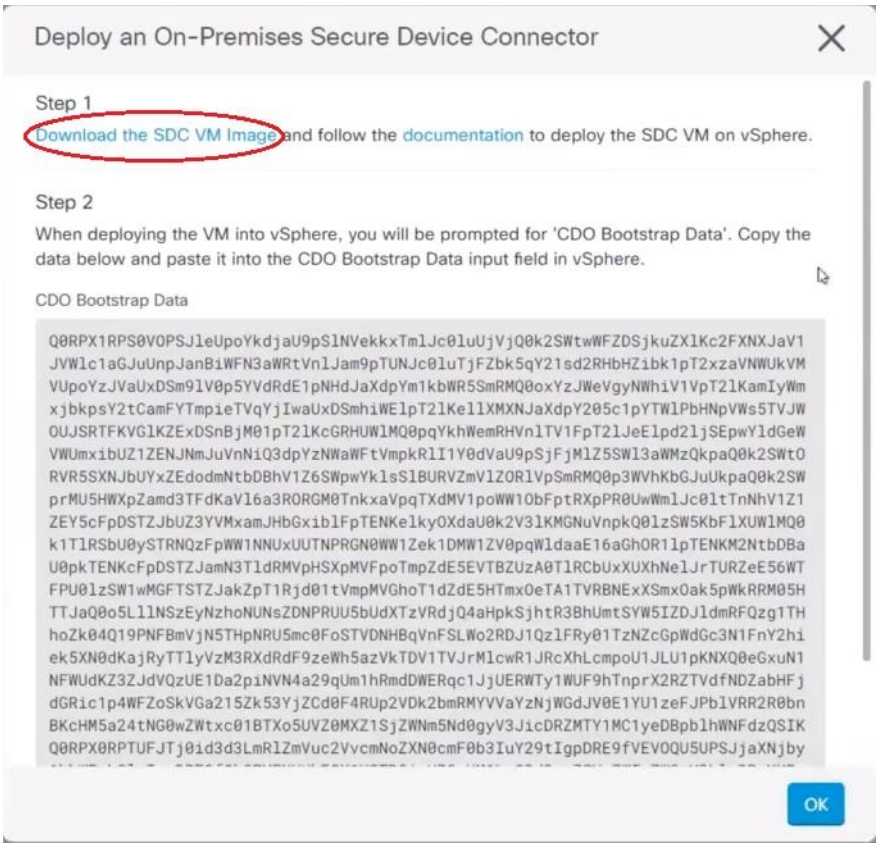
- The SDC virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

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 cdo 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
```

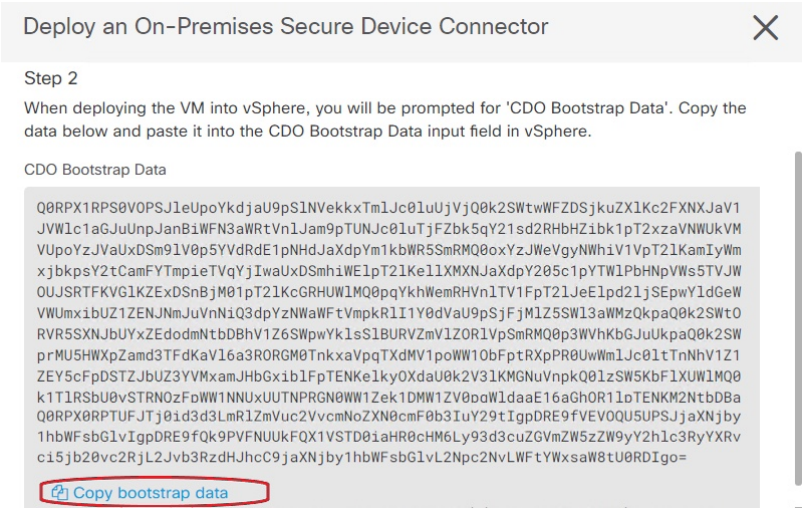
Step 23 When prompted with **[sudo] password**, enter the cdo password you created in Step 14.

Step 24 When prompted with **Please copy the bootstrap data form 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 own 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 26 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 10 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 Cisco Defense Orchestrator 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.
- 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 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 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

•

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 Cisco Defense Orchestrator 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

•

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) and CDO.
- Review Connect Cisco Defense Orchestrator 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 own VM, on page 13 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.

- **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 From the CDO menu, 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 From the CDO menu, 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.

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 in order 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 ~]$
```

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 own 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 sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

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

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

Devices, Software, and Hardware Supported by CDO

Cisco Defense Orchestrator (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.

Browsers Supported in CDO

CDO supports the latest version of these browsers:

- Google Chrome
- Mozilla Firefox

CDO Platform Maintenance Schedule

CDO Maintenance Schedule

CDO updates its platform every week with new features and quality improvements. Updates can be made during a 3 hour period according to this schedule.

Table 1: CDO Maintenance Schedule

Day of the Week	Time of Day (24-hour time)
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, you can access that platform as well. Additionally, the devices you have onboarded to CDO continue to enforce their security policies.

Note We advise you not to use CDO to deploy configuration changes on the devices it manages during maintenance periods.

If there is a failure 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.

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.

The update to your tenant may take up to 1 hour and occurs within the 3 hour maintenance period on the maintenance day assigned to your tenant's region. While your tenant is being updated, you will not be able to

access the cloud-delivered Firewall Management Center environment, but you will still be able to access the rest of CDO.

Table 2: Cloud-delivered Firewall Management Center Maintenance Schedule

Day of the Week	Time of Day (24-hour time)	Region
Wednesday	04:00 UTC - 07:00 UTC	Europe, the Middle East, or Africa (EMEA)
Wednesday	17:00 UTC - 20:00 UTC	Asia-Pacific-Japan (APJ)
Thursday	09:00 UTC - 12:00 UTC	Americas

Manage a CDO Tenant

Cisco Defense Orchestrator (CDO) gives you the ability to customize certain aspects of your tenant and individual user accounts on the Settings page. From the CDO menu bar, click **Settings** in the left navigation panel.

General Settings

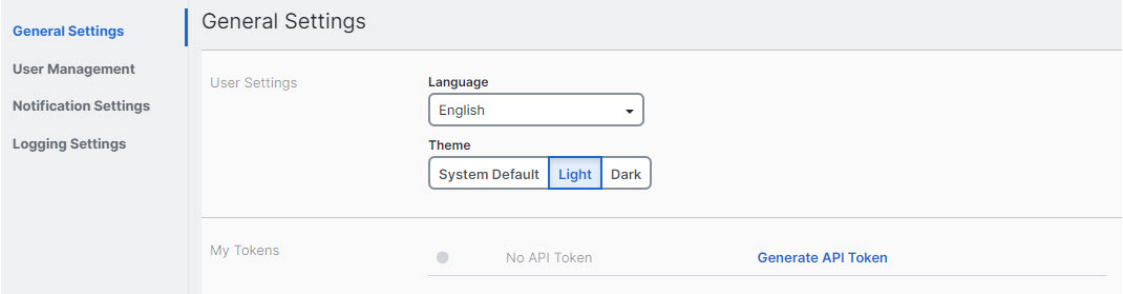
From the admin drop-down in the upper right, click **Settings**.

See the following topics regarding general CDO Settings:

- User Settings, on page 39
- For **My Tokens**, see API Tokens, on page 47
- For **Tenant Settings**, see:
  - Enable Change Request Tracking, on page 40
  - Prevent Cisco Support from Viewing your Tenant, on page 40
  - Default Conflict Detection Interval, on page 41
  - Web Analytics, on page 41
  - Tenant ID, on page 41
  - Tenant Name, on page 41

User Settings

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



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 admin drop-down in the upper right, click **Settings**.

Step 2 Click the **General** tab.

Step 3 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 admin drop-down in the upper right, click **Settings**.

Step 2 Click the **General** tab.

Step 3 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 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 From the admin drop-down in the upper right, click **Settings**.

Step 2 Click the **General** tab.

Step 3 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 admin drop-down in the upper right, click **Settings**.

Step 2 Click the **General Settings** tab.

Step 3 Click the drop-down menu for **Default Conflict Detection Interval** and select a time value.

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 admin drop-down in the upper right, click **Settings**.

Step 2 Click the **General Settings** tab.

Step 3 Click the slider under **Web Analytics**.

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).

Tenant Notification Settings

Notifications are generated by CDO 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. While these notifications are applied to all the devices associated with your tenant, not all device types support all of the available options. For example, background log search is only applicable for tenants who signed up for event logging.

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

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 42 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. For more information on how Webex Teams handles webhooks, see Webex for Developers for more information.

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

Step 1 Open the Webex Teams application.

Step 2 In the lower left corner of the window, click the **Apps** icon. This action opens the Cisco Webex App Hub in new tab in your preferred browser.

Step 3 Use the search bar to find **Incoming Webhooks**.

Step 4 Select **Connect**. This action opens an OAuth Authorization to allow the application in a new tab.

Step 5 Select **Accept**. The tab automatically redirects to the application's configuration page.

Step 6 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 **Space**. The Space must already exist in Webex team. 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.

Step 7 Select **Add**. The Webex Space you chose will receive a notification that the application is added.

Step 8 Copy the Webhook URL.

Step 9 Log into CDO.

Step 10 From the navigation bar to the left, click **Settings** > **Notification Settings**.

Step 11 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 12 Scroll to **Service Integrations**.

Step 13 Click the blue plus button.

Step 14 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 15 Expand the drop-down menu and select **Webex** as the Service Type.

Step 16 Paste the webhook URL that you generated from the service.

Step 17 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 Cisco Defense Orchestrator

Cisco Defense Orchestrator (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 Cisco Defense Orchestrator User Records

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 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 Cisco Defense Orchestrator 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 such as tiles representing https://defenseorchestrator.com or https://defenseorchestrator.eu or https://www.apj.cdo.cisco.com/.

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 Cisco Defense Orchestrator, 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.

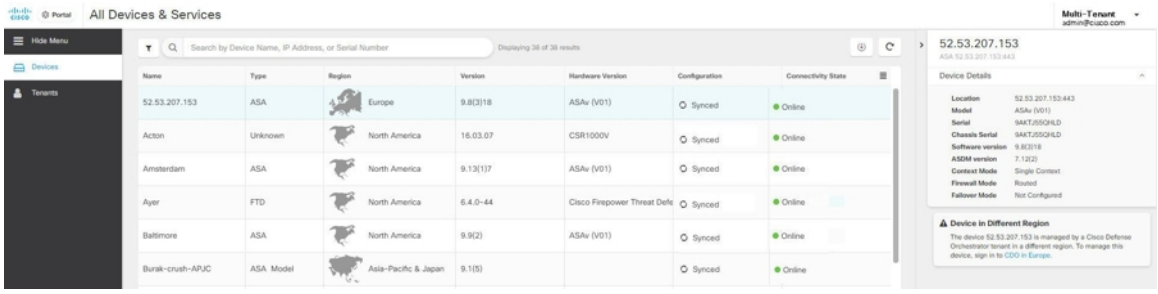
We recommend you clearing cache and cookies from your web browser to avoid certain browser-related issues that may occur.

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.

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 From the navigation bar to the left, 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 Go to the portal and click the **Tenants** tab.

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

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

Manage-Tenant Portal Settings

Cisco Defense Orchestrator (Defense Orchestrator) gives you the ability 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 navigation bar to the left.

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 Cisco Defense Orchestrator User Records to learn how the identity provider (IdP) account and the user record interact. CDO users need a CDO record and a corresponding IdP account so they can be authenticated and access your CDO tenant.

Unless your enterprise has it's 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 temporarily associated with your account to resolve a support ticket.

View the User Records Associated with your Tenant

From the CDOnavigation bar, click **Settings** > **User Management**.

Note To prevent Cisco support from accessing your tenant, configure your Account Settings 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 user(s), 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 AD group from the User Management page. See User Roles in CDO for more information.

Active Directory Groups Tab

The User Management section of the **Settings** page has a tab for Active Directory Groups that are currently mapped to CDO. Most importantly, this page displays the role of the AD group as assigned in your AD manager.

Users within an AD group are not listed individually in either the Active Directory Groups tab or the Users tab.

Audit Logs Tab

The User Management section of the **Settings** page has a tab for Audit Logs. This new section shows the last time of login of all users who accessed a CDO tenant, and the role(s) each user held at the time of last login. This includes both explicit user logins and AD group logins.

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 AD, and each of those groups can be defined in CDO with different CDO roles. The final permissions a user gets on login are a combination of the roles of all the AD groups defined in CDO that the user is part of. For instance, if a user is part of two AD 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.

AD group mappings only need to be defined once in CDO, and managing access and permissions for users can subsequently be achieved exclusively in AD by adding, removing, or moving users between different groups.

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

Before You Begin

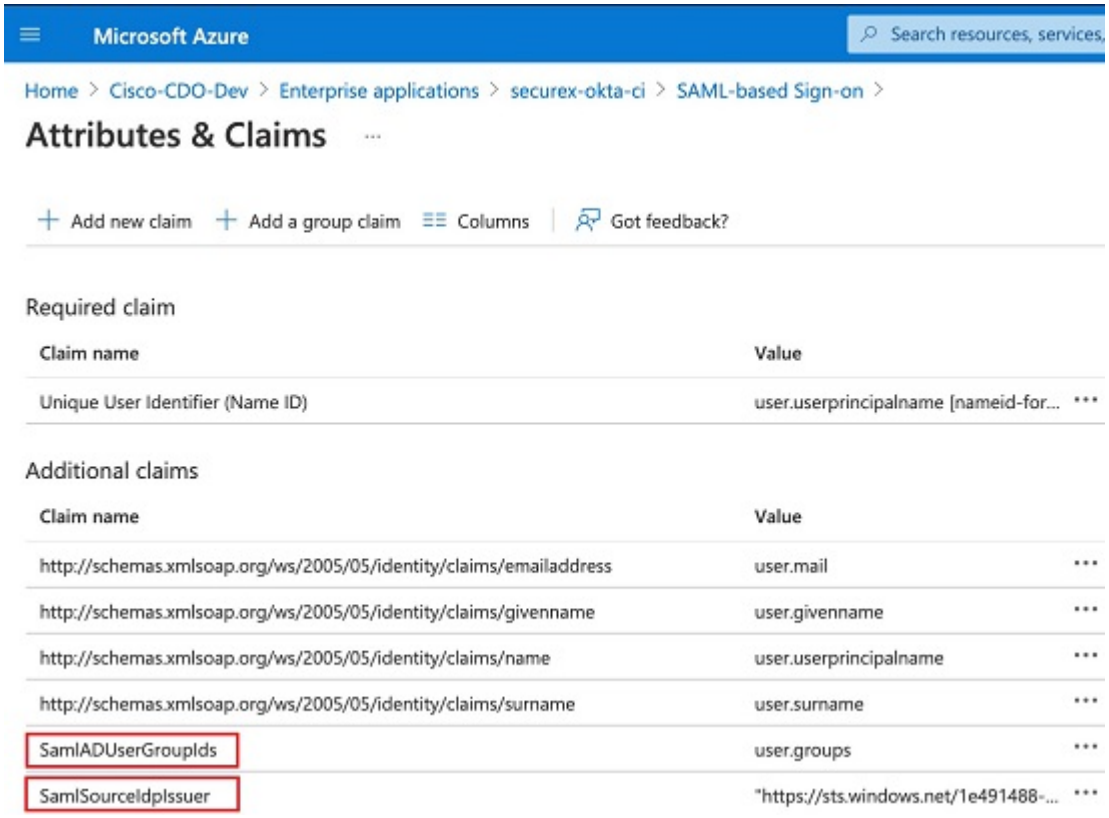
Prior to adding an AD group mapping to CDO as a form of user management, you must have your AD integrated with SecureX. If your AD Identity Provider (IdP) is not already integrated, open a Support Case with Cisco TAC and request a custom AD IdP integration with the following information:

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

After your AD integration is complete, add the following custom SAML claims in your AD. The SAML claims and attributes are required, for you to be able to successfully sign in to your CDO tenant after your AD integration is done. Note that these values are case sensitive:

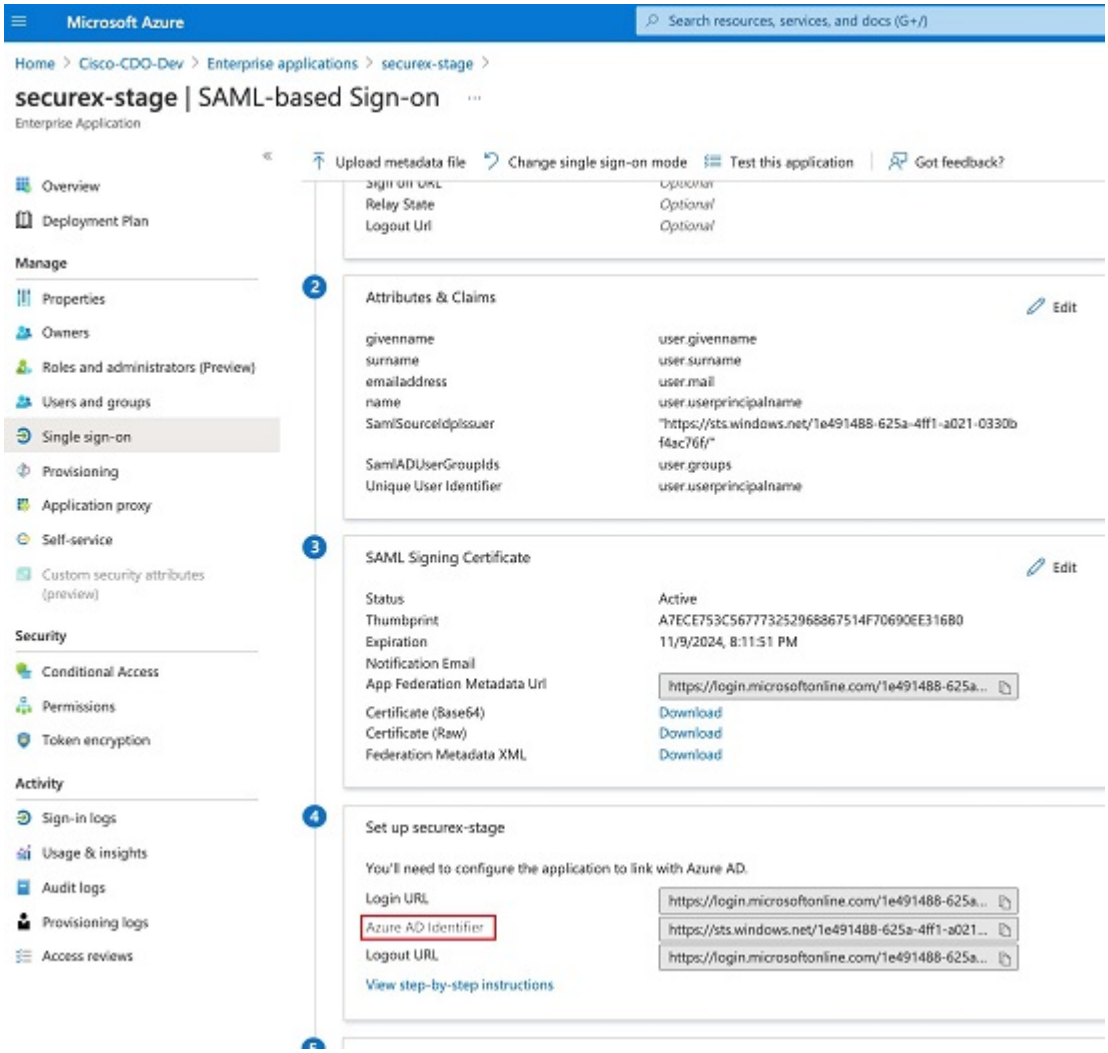
- **SamlADUserGroupIds** - This attribute describes all group associations a user has on AD. For example, in Azure select + **Add a group claim** as seen in the screenshot below:

  Figure 1: Custom Claims defined in Active Directory



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

Figure 2: Locate the Azure Active Directory Identifier



Add an Active Directory Group for User Management

Step 1 Log in to CDO.

Step 2 From the admin drop-down in the upper right, click **Settings**.

Step 3 Click the **User Management** tab.

Step 4 Select the **Active Directory Groups** tab at the top of the table.

Step 5 If there are no current AD groups, click **Add AD group**. If there are existing entries, click the Add button.

Step 6 Enter the following information:

- **Group Name** - Enter a unique name. This name does not have to match the group name in your AD. CDO does not support special characters for this field.

- **Group Identifier** - Manually enter the Group Identifier from your AD. 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 AD Issuer value from your AD.
- **Role** - This determines the role for all the users included in this AD group. See User Roles for more information.
- (Optional) **Notes** - Add any notes that are applicable to this AD group.

Step 7 Select **OK**.

Edit an Active Directory Group for User Management

Before you begin

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

Step 1 Log in to CDO.

Step 2 From the admin drop-down in the upper right, click **Settings**.

Step 3 Click the **User Management** tab.

Step 4 Select the **Active Directory Groups** tab at the top of the table.

Step 5 Identify the AD Group you want to edit and select the **Edit** icon.

Step 6 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 AD. 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 AD Issuer value from your AD.
- **Role** - This determines the role for all the users included in this AD group. See User Roles for more information.
- **Notes** - add any notes that are applicable to this AD group.

Delete an Active Directory Group for User Management

Step 1 Log in to CDO.

Step 2 From the admin drop-down in the upper right, click **Settings**.

Step 3 Click the **User Management** tab.

Step 4 Select the **Active Directory Groups** tab at the top of the table.

Step 5 Identify the AD Group you want to delete.

Step 6 Select the **Delete** icon.

Step 7 Click **OK** to confirm you want to delete the AD group.

Create a New CDO User

These two tasks are required to create a new CDO user. They do not need to be performed sequentially:

- Create a Cisco Security Cloud Sign On Account for the New User
- Create a CDO 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 at any time by the new user themselves. They do not need to know the name of the tenant they will be assigned to.

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 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.

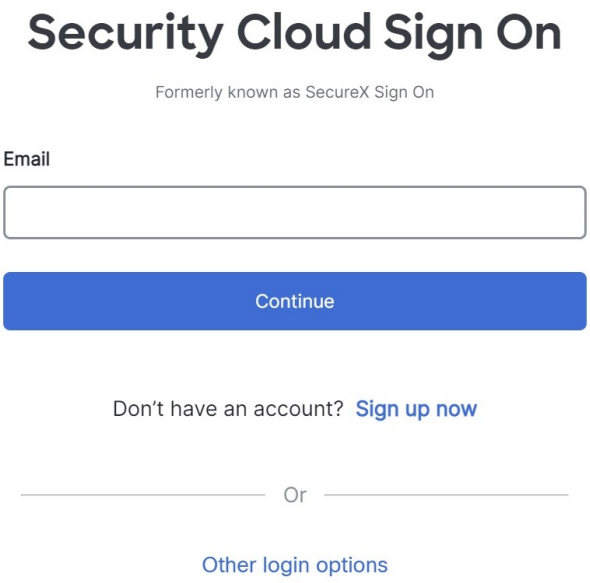
Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication

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

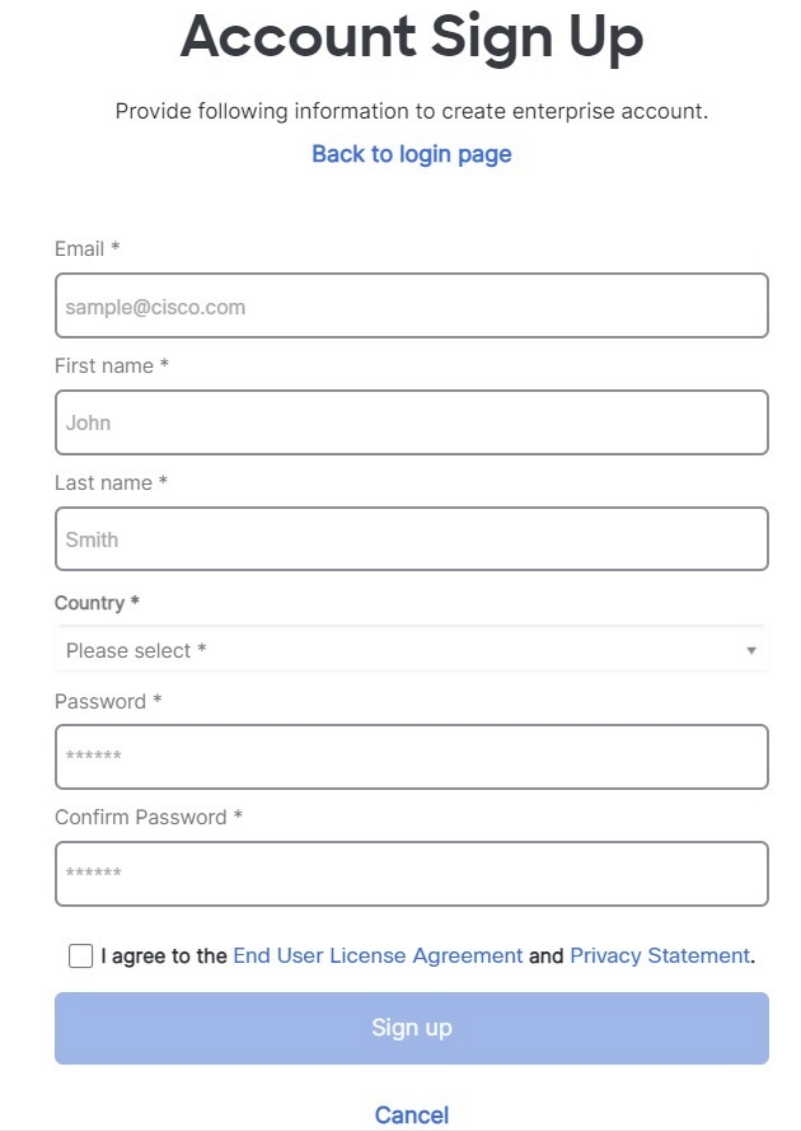
Step 1 **Sign Up for a New Cisco Security Cloud Sign On Account**.

a. Browse to https://sign-on.security.cisco.com.

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



c. Fill in the fields of the Create Account dialog.



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. After you click **Create Account**.

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 CDO User Record with Your CDO Username

Only a CDO user with "Super Admin" privileges can create the CDO user record. The Super Admin should 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 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 **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 Cisco Defense Orchestrator (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**.

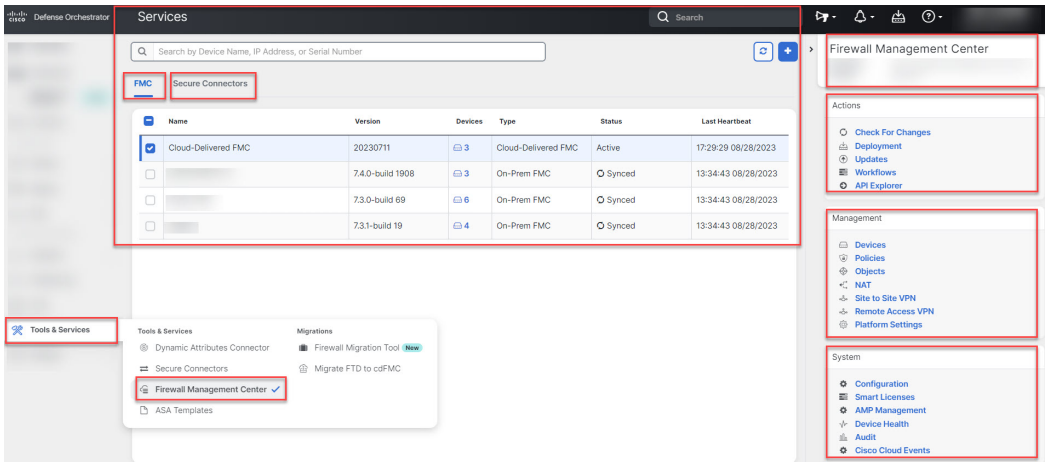
Step 5 Confirm that you want to remove the account from the tenant by clicking OK.

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

Cisco Defense Orchestrator (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 79.
- 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 81.
- 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 (CDO) 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 navigation bar, 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 78

• Bulk Reconnect Devices to CDO, on page 78

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 From the navigation bar, 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.

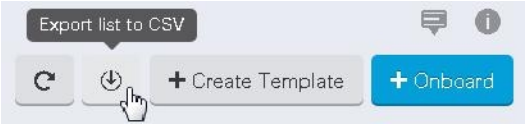
Step 1 In the CDO navigation bar, click **Inventory**.

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 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.

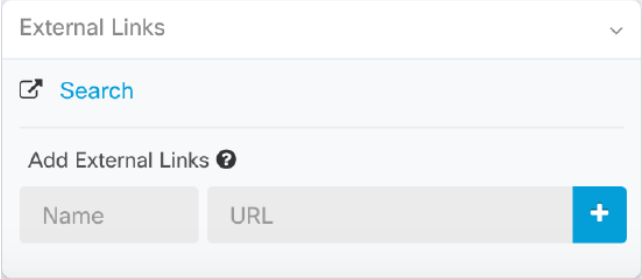
Step 4 Select the device you want so it is highlighted.

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 (). 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}
```

.

Related Information:

- Write a Device Note, on page 78
- Export a List of Devices and Services, on page 74

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

Here is a convenient way to open , 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 .

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.

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.

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.

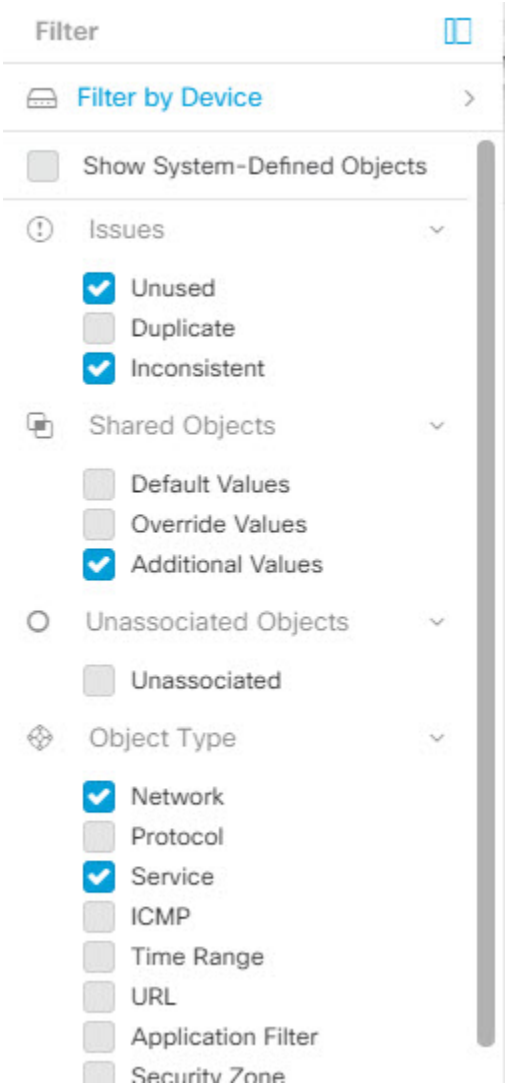
To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

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.

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 AND Objects of type Network OR Service.



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 83.

- 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 Log into CDO using an account with Admin or Super Admin privileges.

Step 2 From the menu bar, navigate to **Settings** > **General Settings**.

Step 3 In Global Search, click **Initiate Full Indexing** to trigger indexing.

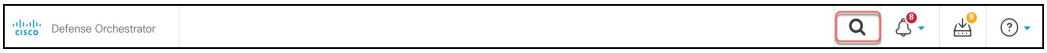
Note Initiating full indexing clears existing indexing of the CDO tenant.

Step 4 Click **here** to view the global search workflow.

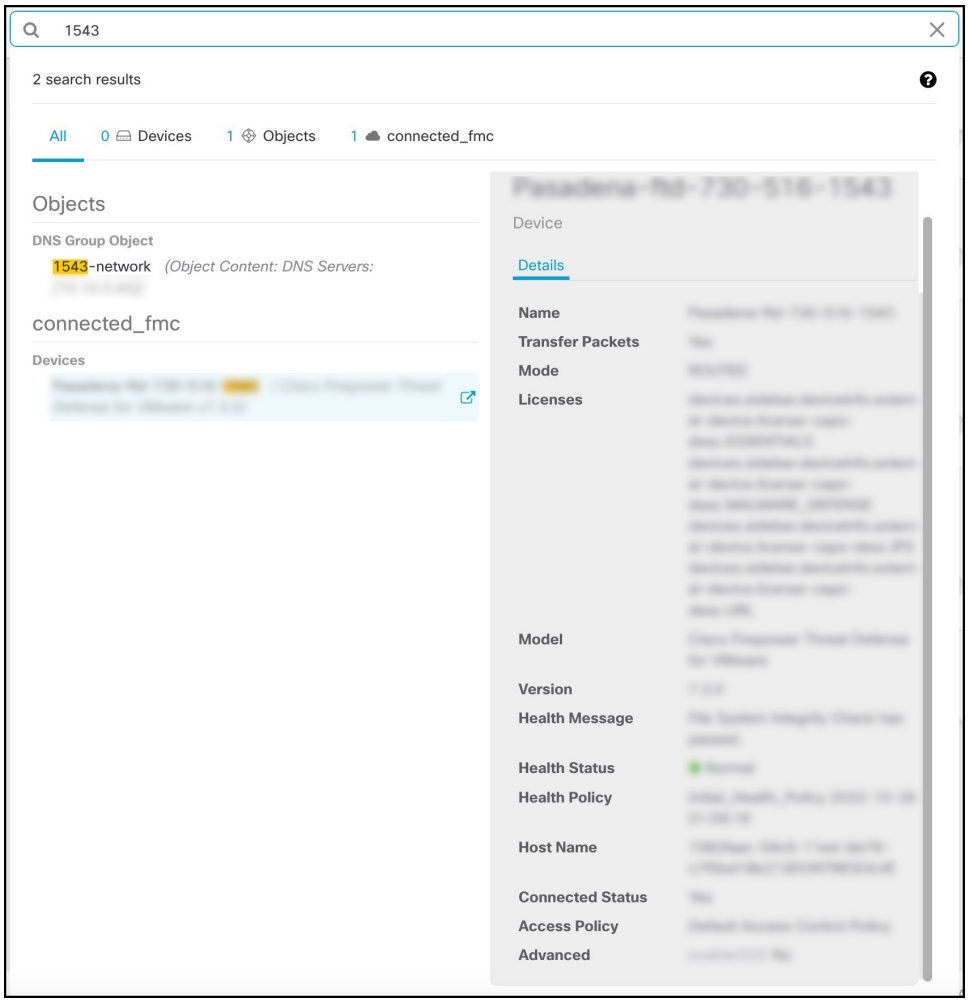
Perform a Global Search

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.



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, and connected_fmc. 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.

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.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Cisco Defense Orchestrator, on page 154 for more information.

Object Types

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

Table 3: On-Premises Secure Firewall Management Center Object Types

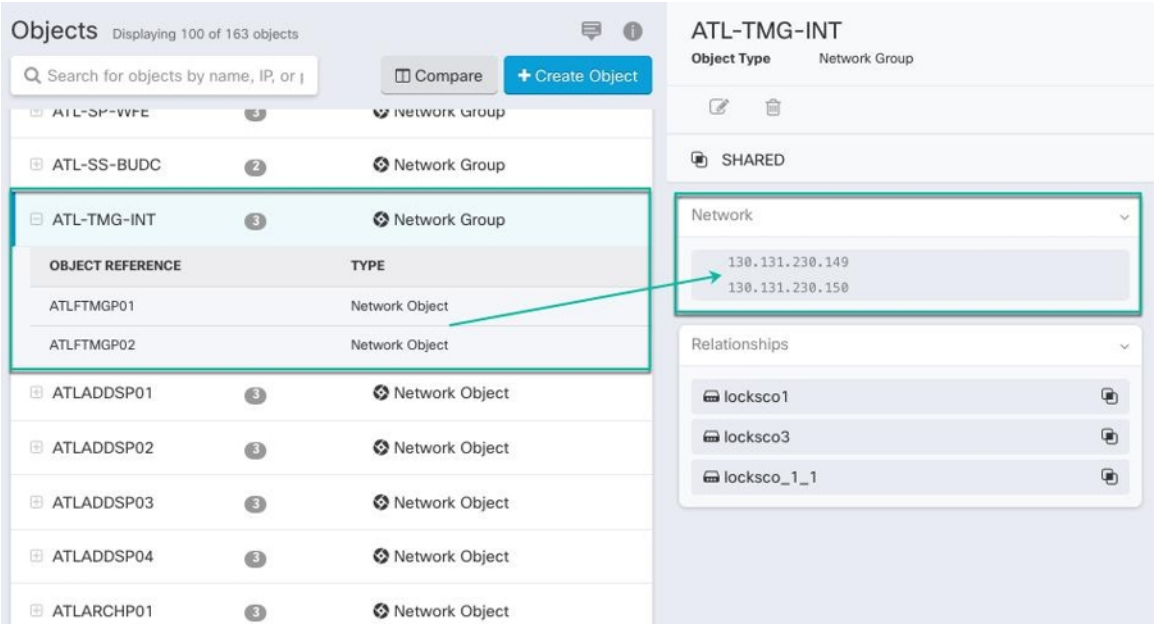
Object	Description
Network Objects	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
Service Objects	Service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the TCP/IP protocol suite.

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.

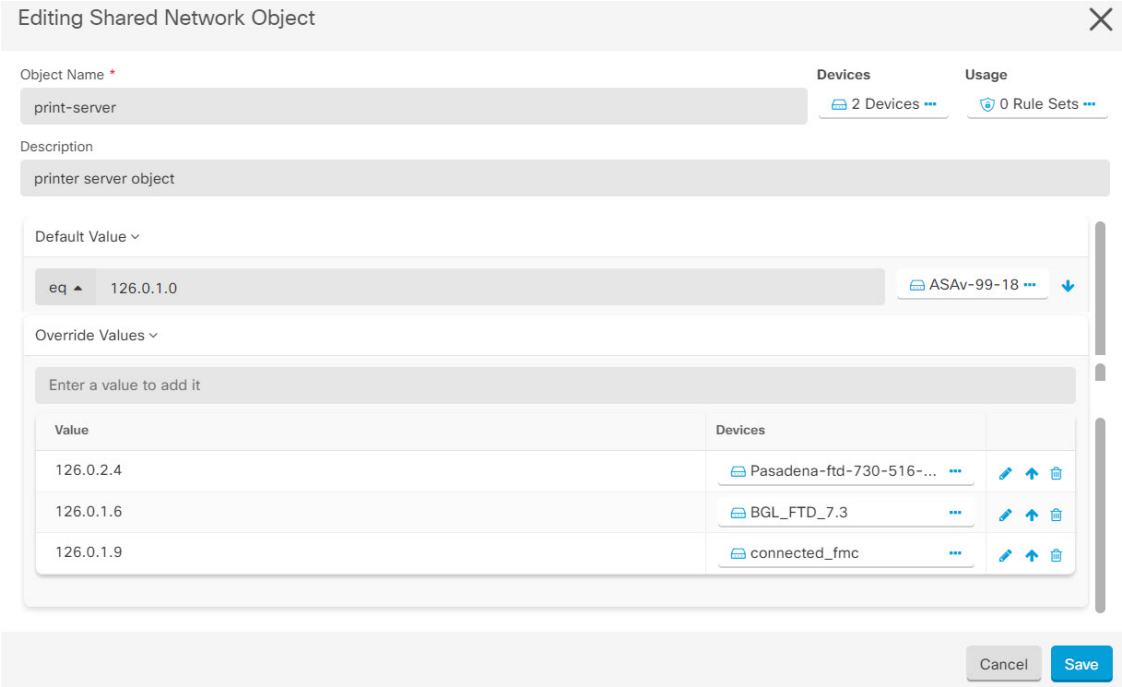


Object Overrides

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.



Note If there are inconsistent objects, you can combine them into a single shared object with overrides. See Resolve Inconsistent Object Issues, on page 160 for more information.

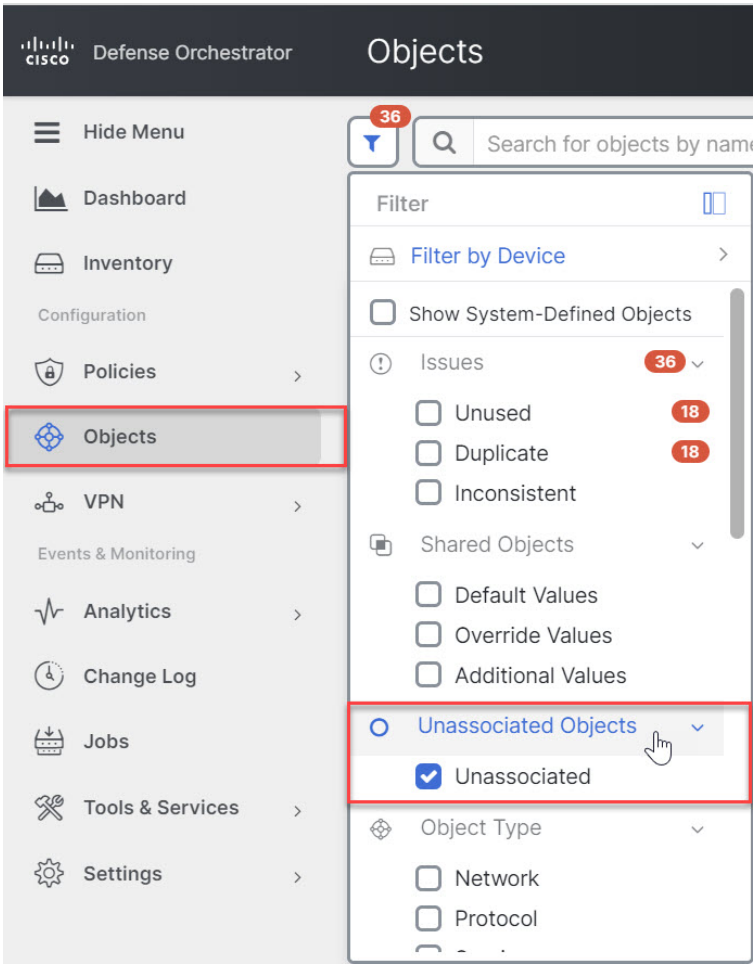
Unassociated Objects

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 CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Filter the objects on the page to find the objects you want to compare.

Step 3 Click the **Compare** button Compare.

Step 4 Select up to three objects to compare.

Step 5 View the objects, side-by-side, at the bottom of the screen.

- Click the up and down arrows in the Object Details title bar to see more or less of the Object Details.

- Expand or collapse the Details and Relationships boxes to see more or less information.

Step 6 (Optional) The Relationships box shows how an object is used. It may be associated with a device or a policy. If the object is associated with a device, you can click the device name and then click **View Configuration** to see the configuration of the device. 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.

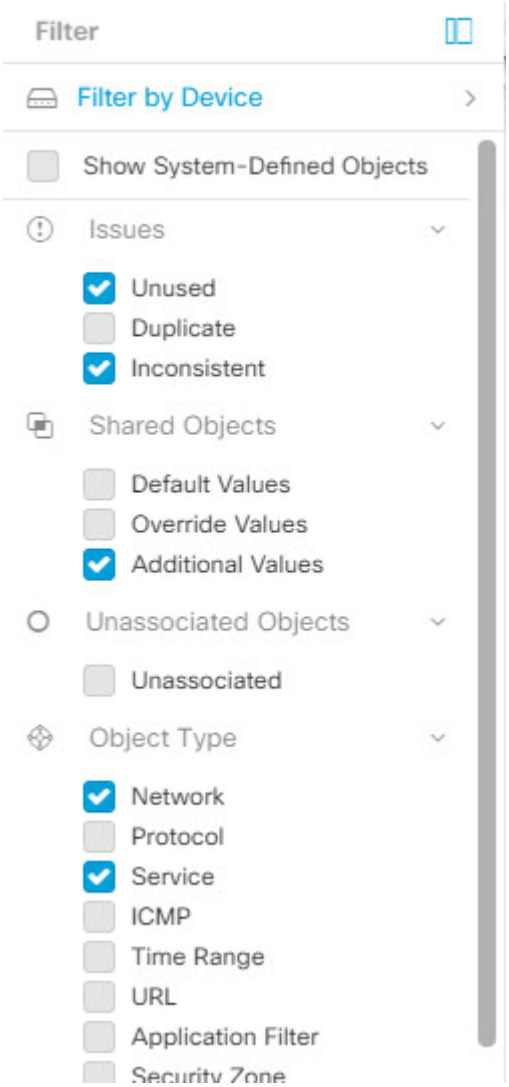
To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

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.

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 AND Objects of type Network OR Service.



Object Filters

To filter, click in the left-hand pane of the Objects tab:

- **All Objects** – This filter provides you all the objects available from all the devices you have on-boarded in CDO. This filter is useful to browse all your objects, or as a starting point to search or further apply sub-filters.
- **Shared Objects** – This quick filter shows you all the Objects that CDO has found to be shared on more than one device.
- **Objects By Device** – Lets you pick a specific device so that you can see objects found on the selected device.

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 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 Objects is **off** by default. To display system objects in the object table, check **Show System 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 CDO navigation bar on the left, 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 CDO navigation bar on the left, 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 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 CDO navigation bar on the left, 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.

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 4: 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 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 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 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 CDO navigation bar on the left, 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 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 CDO navigation bar on the left, 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 122.

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 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 CDO navigation bar on the left, 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 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 CDO navigation bar on the left, 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 122.

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 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 CDO navigation bar on the left, 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 122.

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 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 CDO navigation bar on the left, 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 122.

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

Create or Edit a Firepower Network Object or Network Groups

A Firepower network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects and network groups that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Cisco Defense Orchestrator (CDO).

Firepower network objects and groups can be used by ASA, threat defense, FDM-managed, and Meraki devices. See Reusing Network Objects Across Products, on page 94.

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

When you create a network object or group on the 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 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.

Table 5: IP addresses that can be added to network objects

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

Related Information:

- Create a Firepower Network Object, on page 102
- Edit a Firepower Network Object, on page 104
- Add Additional Values to a Shared Network Group, on page 106
- Edit Additional Values in a Shared Network Group, on page 108

Create a Firepower Network Object

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

When you create a network object or group on the 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

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

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

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

Step 6 In the **Value** section:

- Select **eq** and enter a single IP address, a subnet address expressed in CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and enter an IP address range.

Note Do not set a host bit value. If you enter a host bit value other than 0, CDO unsets it while creating the object, because the cloud-delivered Firewall Management Center only accepts IPv6 objects with host bits not set.

Step 7 Click **Add**.

Attention: The newly created network objects aren't associated with any FDM-managed device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters. For more information, see

Configure Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create a Firepower Network Group

A **network group** can contain network objects and network groups. When you create a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group.

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

When you create a network object or group on the 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

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

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

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

Step 6 In the **Values** field, enter a value or name. When you start typing, CDO provides object names or values that match your entry.

Step 7 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 8 If 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 9 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Note: You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.

Step 10 After adding the required objects, click **Save** to create a new network group.

Step 11 Preview and Deploy Configuration Changes for All Devices.

Edit a Firepower Network Object

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

Changes you make to network objects and groups on the 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the network object and click the edit icon in the **Actions** pane.

Step 4 Edit the values in the dialog box in the same fashion that you created them in "Create a Firepower Network Group".

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

Step 5 Click **Save**. 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 a Firepower Network Group

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

Changes you make to network objects and groups on the 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the network group you want to edit by using object filters and search field.

Step 3 Select the network group and click the edit icon in the **Actions** pane.

Step 4 Change the object name and description if needed.

Step 5 If you want to change the objects or network groups that are already added to the network group, perform the following steps:

a. Click the edit icon appearing beside the object name or network group to modify them.

b. Click the checkmark to save your changes. **Note**: You can click the remove icon to delete the value from a network group.

Step 6 If you want to add new network objects or network groups to this network group, you have to perform the following steps:

a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, 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.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 7 Click **Save**. CDO displays the policies that will be affected by the change.

Step 8 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 9 Preview and Deploy Configuration Changes for All Devices.

Add an Object Override

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

Changes you make to network objects and groups on the 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object to which you want to add an override, using object filters and search field.

Step 3 Select the network object and click the edit icon in the **Actions** pane.

Step 4 Enter the value in the **Override Values** dialog box and click **+ Add Value**.

Important The override you are adding must have the same type of value that the object contains. For example, to a network object, you can configure an override only with a network value and not a host value.

Step 5 Once you see that the value is added, click the cell in the **Devices** column in **Override Values**.

Step 6 Click **Add Devices**, and choose the device to which you want the override to be added. The device you select must contain the object to which you are adding the override.

Step 7 Click **Save**. CDO displays the devices that will be affected by the change.

Step 8 Click **Confirm** to finalize the addition of the override to the object and any devices affected by it.

Note You can add more than one override to an object. However, you must select a different device, which contains the object, each time you are adding an override.

Step 9 See Object Overrides, on page 87 to know more about object overrides and Edit Object Overrides , on page 106 to edit an existing override.

Edit Object Overrides

You can modify the value of an existing override as long as the object is present on the device.

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Locate the object having override you want to edit by using object filters and search field.

Step 3 Select the object having override and click the edit icon in the Actions pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click on the cell in the **Devices** column in **Override Values** to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Override Values** to push and make it as the default value of the shared object.
- Click the delete icon next to the override you want to remove.

Step 5 Click **Save**. 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.

Add Additional Values to a Shared Network Group

The values in a shared network group that are present on all devices associated with it are called "default values". 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 in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory". These two servers do not participate in determining whether the object "Active-Directory" is consistent or

shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

Note If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See Resolve Inconsistent Object Issues, on page 160 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 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the shared network group you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

- The **Devices** field shows the devices the shared network group is present.
- The **Usage** field shows the rulesets associated with the shared network group.
- The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.

Step 4 In the **Additional Values** field, enter a value or name. When you start typing, 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.

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.

Edit Additional Values in a Shared Network Group

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

Changes you make to network objects and groups on the 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 CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object having the override you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
- Click arrow in **Override Values** to push and make it as default objects of the shared network group.
- Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. 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.

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

Discover and Manage On-Prem Firewall Management Center Network Objects

If you have an On-Prem Firewall Management Center that you manage using CDO and you want to share and manage its objects, do the following:

Step 1 From the CDO menu, navigate **Tools & Services** > **Firewall Management Center** to view the **Services** page.

Step 2 If you already have onboarded an on-prem management center to CDO, select it.

If you want to onboard a new on-prem management center, see Onboard an On-Prem Firewall Management Center.

Step 3 Choose **Settings** from the **Actions** pane on the right. Note that you do not get to see the **Actions** pane when you select more than one on-prem management center.

Note You must be an admin or a super admin to be able to use **Settings**.

Step 4 Enable the **Discover & Manage Network Objects** toggle button. If you want your changes to be automatically synchronized with on-prem management center and not staged for review, turn the **Enable automatic sync of network objects** toggle on.

Note
- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-prem management center that you have selected has one or more child domains or has the Chanage Management workflow enabled on it..
- You cannot turn the **Enable automatic sync of network objects** toggle on if the **Discover & Manage Network Objects** toggle is turned off.

For every new on-prem management center onboarded to CDO, this toggle button needs to be enabled manually. Once you enable this option, CDO starts to discover objects from your on-prem management center, which you can share, manage, and use to set consistent object definitions across other platforms managed by CDO.

In CDO, when you add overrides to objects that are discovered from an on-prem management center and push the changes back to the on-prem management center, these objects start accepting overrides in the on-prem management center even if they were not accepting overrides before—the **Allow Overrides** checkbox in **View Network Object** window is checked automatically when an override is added from CDO.

Note If you want to assign already-existing objects in CDO to your on-prem management center, choose the on-prem management center and click **Assign Objects** from the **Actions** pane.

Related Information

- Network Objects
- Preview and Deploy On-Prem Firewall Management Center Configurations
- Enable Conflict Detection for an On-Prem Firewall Management Center, on page 127

Service Objects

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

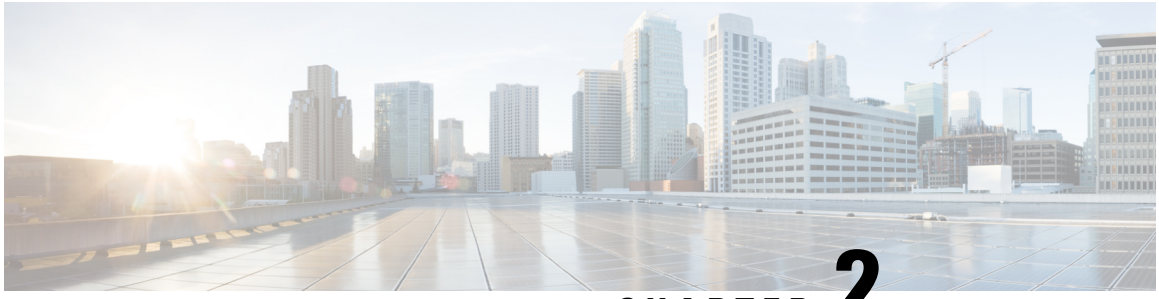
An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. CDO recognizes these objects in ASA and Firepower configurations when those devices are onboarded and CDO gives them their own filter of "ICMP" so you can find the objects easily.

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 92



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 an On-Prem Management Center, on page 111
- Remove an On-Prem Firewall Management Center from CDO, on page 117

Onboard an On-Prem Management Center

Review Connect Cisco Defense Orchestrator to your Managed Devices, on page 9 for more information.

Note 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.

Limitations and Guidelines

These are the limitations applicable to onboarding an On-Prem Management Center:

- Onboarding an On-Prem Management Center also onboards all of the devices registered to the On-Prem Management Center. Be aware that if a managed device is disabled, or unreachable, CDO may display the device in the **Inventory** page, but cannot successfully send requests or view device information.
- We recommend creating a new user on the On-Prem Management Center specifically for CDO communication that has administrator-level permissions. If you onboard an On-Prem Management Center and then simultaneously log into that On-Prem Management Center with the same login credentials, onboarding fails.
- If you create a new user on the On-Prem Management Center for CDO communication, the **Maximum Number of Failed Logins** for the user configuration must be set to "0".

Network Requirements

Before you onboard a device, ensure the following ports have external access. If communication ports are blocked behind a firewall, onboarding the device may fail.

Port	Protocol/Feature	Platforms	Direction	Details
7/UDP	UDP/audit logging	FMC	Outbound	Verify connectivity with the syslog server when configuring audit logging.
25/tcp	SMTP	FMC	Outbound	Send email notices and alerts.
53/tcp 53/udp	DNS	FMC	Outbound	DNS
67/udp 68/udp	DHCP	FMC	Outbound	DHCP
80/tcp	HTTP	FMC	Outbound	Display RSS feeds in the dashboard.
80/tcp	HTTP	FMC	Outbound	Download or query URL category and reputation data (port 443 also required).
80/tcp	HTTP	FMC	Outbound	Download custom Security Intelligence feeds over HTTP.
123/udp	NTP	FMC	Outbound	Synchronize time.
162/udp	SNMP	FMC	Outbound	Send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	FMC	Outbound	Communicate with an LDAP server for external authentication. Obtain metadata for detected LDAP users (FMC only). Configurable.
443/tcp	HTTPS	FMC	Inbound	Allow inbound connection to port 443 if you are onboarding the FMC with an on-premises Secure Device Connector.
443/tcp	HTPS	FMC	Outbound	Allow outbound traffic from port 443 if onboarding the FMC to CDO using the cloud connector.
443/tcp	HTPS	FMC	Outbound	Allow outbound connection for port 443 if onboarding the FMC using SecureX.

Port	Protocol/Feature	Platforms	Direction	Details
443/tcp	HTTPS	FMC	Outbound	Send and receive data from the internet.
443	HTTPS	FMC	Outbound	Communicate with the AMP cloud (public or private)
514/udp	Syslog (alerts)	FMC	Outbound	Send alerts to a remote syslog server.
1812/udp 1813/udp	RADIUS	FMC	Outbound	Communicate with a RADIUS server for external authentication and accounting. Configurable.
5222/tcp	ISE	FMC	Outbound	Communicate with an ISE identity source.
6514/tcp	Syslog (audit events)	FMC	Outbound	Send audit logs to a remote syslog server, when TLS is configured.
8305/tcp	Appliance communications	FMC	Both	Securely communicate between appliances in a deployment. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8989/tcp	Cisco Success Network	FMC	Outbound	Transmit usage information and statistics.

Onboard an On-Prem Firewall Management Center to CDO with Credentials

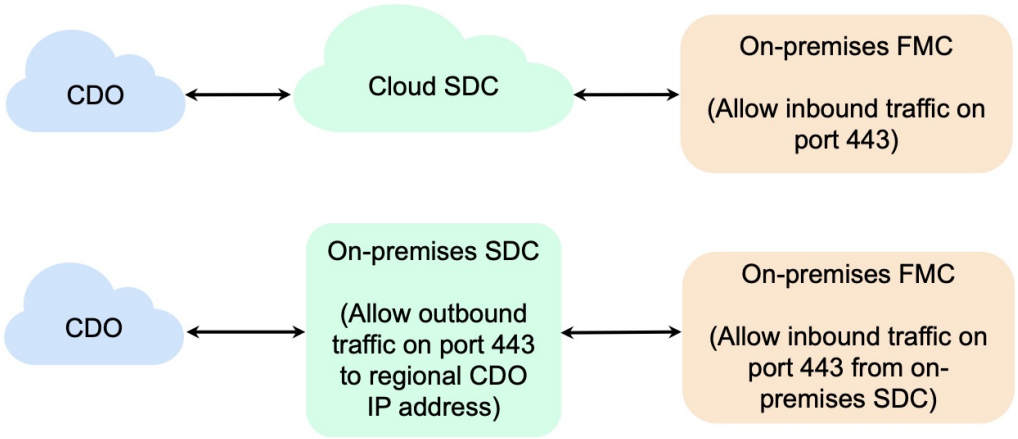
To onboard an On-Prem Firewall Management Center to CDO with credentials, follow this procedure:

Before you begin

Review Onboard an On-Prem Management Center, on page 111.

Make sure you allow proper port access on your on-premises Firewall Management Center:

- Allow inbound connectivity on port 443 if you are onboarding the on-premises FMC using an on-premises Secure Device Connector.
- Allow outbound connectivity on port 443 if you are onboarding the FMC using the Cloud Connector.



Step 1 From the CDO navigation bar, click **Tools & Services** > **Firewall Management Center**.

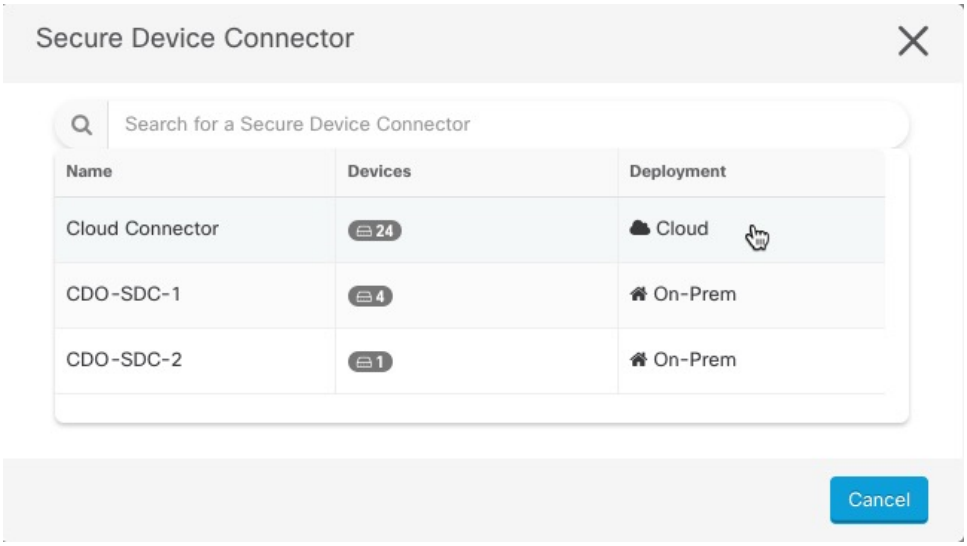
Step 2 Click + to onboard an On-Prem Firewall Management Center.

Step 3 Click **Firewall Management Center**.

Step 4 Select the **Use Credentials** card.

Step 5 Click the **Secure Device Connector** button and select an SDC installed in your network. If you would rather not use an SDC, CDO can connect to your On-Prem Management Center using the Cloud Connector. Your choice depends on how you Connect Cisco Defense Orchestrator to your Managed Devices.

Figure 3: Choose a Secure Device Connector



Step 6 Enter the device name and location. Click **Next**.

Step 7 Enter the **Username** and **Password** of the account credentials you want to use to access the On-Prem Management Center. Click **Next**.

Step 8 The device is onboarded. From here you can opt to add labels to your On-Prem Management Center, or click **Go to Services** to view the page of onboarded devices. If healthy, the FMC is displayed with a **Synced** status.

Note Note that the devices managed by the On-Prem Management Center are automatically named as "*<fmcname>_<manageddevicename>*."

About Auto-Onboarding an On-Prem Firewall Management Center to CDO

As a Super Admin or Admin user on CDO, you can use the platform's auto-onboarding of on-prem management centers functionality. This feature automatically initiates the onboarding process for all on-prem management centers that are running Version 7.2 or later and are linked to your SecureX tenant or registered to the Cisco Security Cloud. Additionally, it also onboards the threat defense devices that are connected to those on-prem management centers.

This feature is enabled by default in CDO, so you can expect all on-prem management centers and threat defense devices to be automatically onboarded, which can significantly enhance efficiency. CDO polls SecureX for new on-prem management centers every hour. It onboards the active on-prem management center high availability (HA) pair.

Note that a new CDO tenant also comes with this feature enabled by default. This feature holds good for you if you have an on-prem management center running Version 7.2 and later and if you fit into one of the following categories:

- Register your on-prem management center through SecureX for the first time and you do not have a CDO tenant
- Auto-onboard an already registered on-prem management center to a new CDO tenant
- Auto-onboard an already registered on-prem management center to an existing CDO tenant

Register your on-prem management center through SecureX for the first time and you do not have a CDO tenant

If you have an on-prem management center that is not registered through SecureX, you can register it to the Cisco Security Cloud through CDO. See Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide for instructions on how to do this. If you do not have a CDO account already, you will be prompted to create one for yourself during the registration process, which your on-prem management center then uses to connect to the Cisco Security Cloud.

Auto-onboard an already registered on-prem management center to a new CDO tenant

If you have an on-prem management center that is already registered through SecureX and when you create a new CDO tenant, because CDO comes with the auto-onboarding of on-prem management centers feature enabled by default, you can expect your on-prem management center to get onboarded to CDO right away. See Create a CDO Tenant for more information.

Auto-onboard an already registered on-prem management center to an existing CDO tenant

If you already have a CDO tenant and an on-prem management center registered with SecureX, and you want to onboard your on-prem management center to CDO for the first time, enable the **Auto onboard On-Prem FMCs using SecureX tenant** toggle.

If you do not see your on-prem management center getting onboarded even after enabling the toggle, make sure again that your CDO and SecureX or Cisco XDR tenant accounts are merged. See Merge Accounts for

instructions. After merging, log out and log in back to your CDO tenant and try disabling and enabling the **Auto onboard On-Prem FMCs using SecureX tenant** toggle.

Auto-Onboard an On-Prem Firewall Management Center with SecureX

Before you begin

Ensure that the following requirements are met:

- The on-prem management center must be running at least Version 7.2.
- SecureX must be enabled on the on-prem management center. See Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide for steps and more information.
- You must allow outbound traffic from port 443 on the on-prem management center.
- The on-prem management center must have a configured module.
- Merge your CDO tenant and SecureX/CTR or Cisco XDR account prior to onboarding your device. See Merge Accounts for instructions.
- After merging your CDO tenant and SecureX/CTR or Cisco XDR, ensure that you log out of your CDO tenant and log in again.

Step 1 Click **Tools & Services** > **Firewall Management Center** > + and choose **FMC**.

Step 2 Click **Discover From SecureX Account** as the method.

The **Auto onboard On-Prem FMCs using SecureX** feature is enabled by default. You can go to **Tools & Services** > **Firewall Management Center** to see the newly onboarded on-prem management centers associated with the SecureX tenant linked to your CDO tenant.

Step 3 You can click the available link to disable this functionality.

Step 4 In the **General Settings** screen, navigate to the **Tenant Settings** section, and disable **Auto onboard On-Prem FMCs using SecureX tenant**.

Note When you disable this functionality, CDO stops further onboarding of the on-prem management center associated with the SecureX tenant. It doesn't remove the already onboarded on-prem management centers. You must manually remove them after disabling the functionality.

Redirect CDO to an On-Prem Firewall Management Center

After you have onboarded an On-Prem Management Center to CDO, you must update the management interface's hostname in the On-Prem Management Center UI to contain the FQDN. If you do not, you cannot cross-launch from CDO.

Use the following procedure to update the management interface hostname and redirect from CDO to the On-Prem Management Center:

Step 1 Log into the On-Prem Management Center UI.

Step 2 Navigate to **System** > **Configuration**.

Step 3 Select the **Management Interfaces** tab.

Step 4 Expand the **Shared Settings** header and click the edit icon.

Step 5 Locate the **Hostname** field and enter the FMC's FQDN.

Step 6 Save changes.

Note: You may have to log out of CDO before you can click **Manage Devices in Firepower Management Center** and cross-launch to the On-Prem Management Center UI.

Remove an On-Prem Firewall Management Center from CDO

If you opt to remove an on-prem management center from CDO, you are also choosing to remove all of the devices managed from CDO. Note that this does **not** remove the on-prem management center from SecureX.

Use the following procedure to remove an on-prem management center and it's registered devices from CDO:

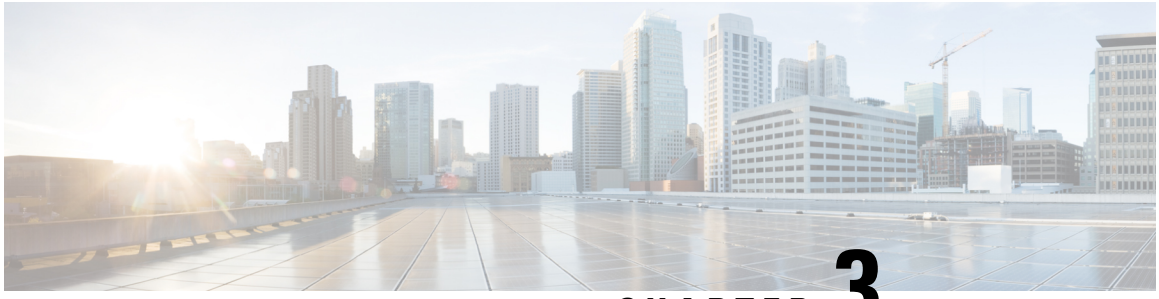
Step 1 In the navigation pane, click **Tools & Services** > **Firewall Management Center**.

Step 2 Ensure the **FMC** tab is selected and choose the on-prem management center you want to remove.

Step 3 In the **Device Actions** pane located to the right, click **Remove On-Prem FMC and its managed devices**.

Step 4 Click **OK** to confirm that you want to remove the on-prem management center and its managed devices from your tenant.

Step 5 Refresh your browser to see an updated list of available devices.



CHAPTER 3

Configuring On-Prem Firewall Management Center Devices

This chapter covers the following sections:

- Discover and Manage On-Prem Firewall Management Center Network Objects, on page 119
- About Device Configuration Changes, on page 120
- Read All Device Configurations, on page 121
- Preview and Deploy Configuration Changes for All Devices, on page 122
- Bulk Deploy Device Configurations, on page 123
- Preview and Deploy On-Prem Firewall Management Center Configurations, on page 124
- Discard Configuration Changes, on page 124
- Discard On-Prem Firewall Management Center Configuration Changes, on page 125
- Out-of-Band Changes on Devices, on page 125
- Synchronizing Configurations Between Defense Orchestrator and Device, on page 126
- Conflict Detection, on page 126
- Automatically Accept Out-of-Band Changes from your Device, on page 127
- Resolve Configuration Conflicts, on page 128
- Schedule Polling for Device Changes, on page 130

Discover and Manage On-Prem Firewall Management Center Network Objects

If you have an On-Prem Firewall Management Center that you manage using CDO and you want to share and manage its objects, do the following:

Step 1 From the CDO menu, navigate **Tools & Services** > **Firewall Management Center** to view the **Services** page.

Step 2 If you already have onboarded an on-prem management center to CDO, select it.

If you want to onboard a new on-prem management center, see Onboard an On-Prem Firewall Management Center.

Step 3 Choose **Settings** from the **Actions** pane on the right. Note that you do not get to see the **Actions** pane when you select more than one on-prem management center.

Note You must be an admin or a super admin to be able to use **Settings**.

Step 4 Enable the **Discover & Manage Network Objects** toggle button. If you want your changes to be automatically synchronized with on-prem management center and not staged for review, turn the **Enable automatic sync of network objects** toggle on.

Note
- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-prem management center that you have selected has one or more child domains or has the Chanage Management workflow enabled on it..
- You cannot turn the **Enable automatic sync of network objects** toggle on if the **Discover & Manage Network Objects** toggle is turned off.

For every new on-prem management center onboarded to CDO, this toggle button needs to be enabled manually. Once you enable this option, CDO starts to discover objects from your on-prem management center, which you can share, manage, and use to set consistent object definitions across other platforms managed by CDO.

In CDO, when you add overrides to objects that are discovered from an on-prem management center and push the changes back to the on-prem management center, these objects start accepting overrides in the on-prem management center even if they were not accepting overrides before—the **Allow Overrides** checkbox in **View Network Object** window is checked automatically when an override is added from CDO.

Note If you want to assign already-existing objects in CDO to your on-prem management center, choose the on-prem management center and click **Assign Objects** from the **Actions** pane.

Related Information

- Network Objects
- Preview and Deploy On-Prem Firewall Management Center Configurations
- Enable Conflict Detection for an On-Prem Firewall Management Center, on page 127

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.

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 notifications tab for the progress of the Read All configurations operation.

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

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

- Preview and Deploy On-Prem Firewall Management Center Configurations, on page 124
- Discard On-Prem Firewall Management Center Configuration Changes, on page 125

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 navigation 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.

Preview and Deploy On-Prem Firewall Management Center Configurations

If you have made configuration changes to an object, for instance, changing a value or adding an override to an object, you can deploy all of those changes at once to your on-prem management center:

Note Note that this task only pushes the configuration changes to the on-prem management center. Ensure you manually deploy these changes to your threat defense devices on your on-prem management center. See Configuration Deployment in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.

Step 1 In the navigation pane, click **Tools & Services** > **Firewall Management Center** and select the On-Prem Firewall Management Center, to which you want to preview and deploy changes.

Note CDO detects that your on-prem management center is out of sync and displays the status as **Not Synced**.

Step 2 Click **Preview and Deploy** on the details pane on the right.

Step 3 Review any warnings and click **Deploy Now**. The deployment starts immediately without a review of the changes. Click **Discard All** if you do not want to proceed with the deploy after previewing.

Step 4 Alternatively, you can also click the button at the top-right of the screen to view the **Devices with Pending Changes** window. Select the devices you want and review the pending changes on the devices that you selected before you deploy them.

Step 5 Click **Deploy Now** to deploy the changes.

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**.

Discard On-Prem Firewall Management Center Configuration Changes

If you want to undo all the configuration changes you made in CDO, for instance to the objects that are shared between your CDO and on-prem management center, use this procedure. Note that when you do this, CDO *completely overwrites* its local copy of the configuration with the configuration stored on the device.

Step 1 In the navigation pane, click **Tools & Services** > **Firewall Management Center**.

Step 2 Select the On-Prem Firewall Management Center, for which you want to discard changes.

Step 3 Click **Discard Changes** in the **Not Synced** pane on the right.

When you click **Discard Changes**, your on-prem management center'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 on-prem management center and the configuration status in CDO returns to **Synced**.

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 Defense Orchestrator 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 Defense Orchestrator 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 Cisco Defense Orchestrator (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 130 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Defense Orchestrator.

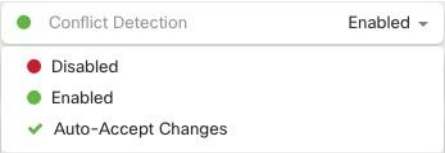
Step 1 In the navigation bar, click **Inventory**.

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.



Enable Conflict Detection for an On-Prem Firewall Management Center

Enabling conflict detection for an On-Prem Firewall Management Center keeps you informed 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.

Step 1 In the navigation bar, click **Tools & Services** > **Firewall Management Center**.

Step 2 From the list, select the on-prem management center for which you want to enable conflict detection.

Step 3 In the **Conflict Detection** box on the right pane, select **Enabled** from the list.

Note Unlike other devices managed by CDO, for an on-prem management center, you can either enable or disable conflict detection; you cannot opt to auto-accept changes.

Automatically Accept Out-of-Band Changes from your Device

You can configure Cisco Defense Orchestrator (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. For on-prem management center, you can do this from the **Services** page by navigating **Tools & Services** > **Firewall Management Center** and selecting the FMC.

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 126 instead.

Configure Auto-Accept Changes

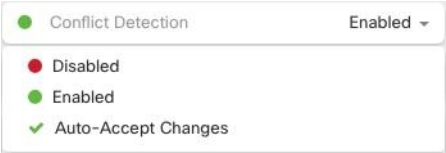
Step 1 Log in to CDO using an account with Admin or Super Admin privileges.

Step 2 From the CDO menu, navigate to **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 From the CDO menu, 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 126 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 126 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:

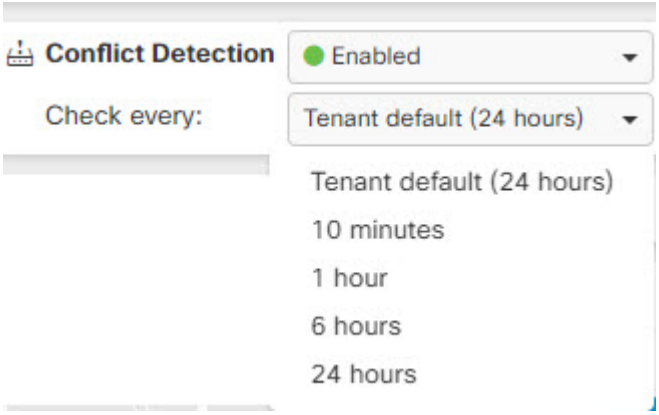
Step 1 In the navigation bar, click **Inventory**.

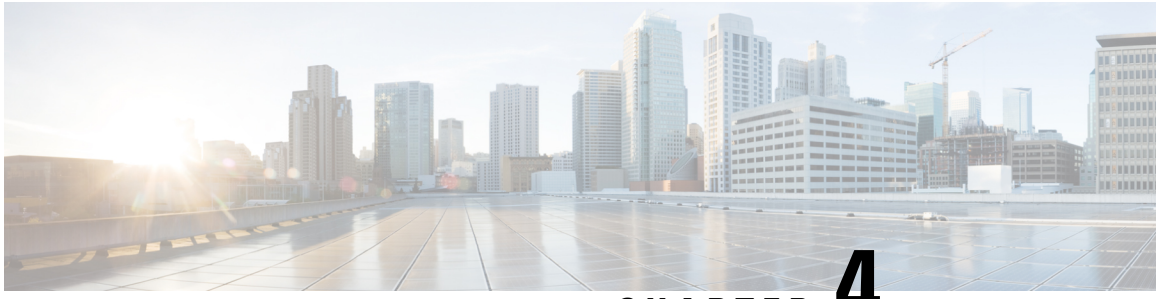
Step 2 Click the **Devices** tab to locate your device.

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:


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours



CHAPTER 4

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, on page 133
- View Change Log Differences, on page 134
- Export the Change Log, on page 135
- Change Request Management, on page 136
- Monitor Workflows in CDO, on page 140

Manage Change Logs in CDO

The Change Log captures configuration changes made in CDO, providing a single view that includes changes in all supported devices and services. These are some of the features of the change log:

- Side-by-side comparison of changes made to device configuration.
- Plain-English labels for all change log entries.
- Records on-boarding and removal of devices.
- Detection of policy change conflicts occurring outside of 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.

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 135 for more information.

Change Log Entries

A change log entry reflects changes to a single device configuration, an action performed on a device, or if a change was made to the device outside of CDO.

- For change log entries that contain a change to configuration, you can expand the change by clicking anywhere in the row.
- For out-of-band changes made outside of CDO that are detected as a conflict, **System User** is reported as the Last User.
- CDO closes a change log entry after the device's configuration on CDO is synced with the configuration on the device or when a device is removed from CDO. Configurations are in sync after "reading" the configuration from the device to CDO or by deploying the configuration from CDO to the device.
- CDO creates a new change log entry immediately after closing an existing entry. Additional configuration changes are added to the open change log entry.
- Events are displayed for read, deploy, and delete actions against a device. These actions close a device's change log.
- A change log is closed once 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 written to 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, those changes are recorded in an **pending** change log entry. Reading a configuration from a device to CDO, deploying changes from CDO to a device, deleting a device from CDO completes, or running a CLI command that updates the running configuration file completes the pending change log and creates a new one for future changes.

Search and Filter Change Log Entries

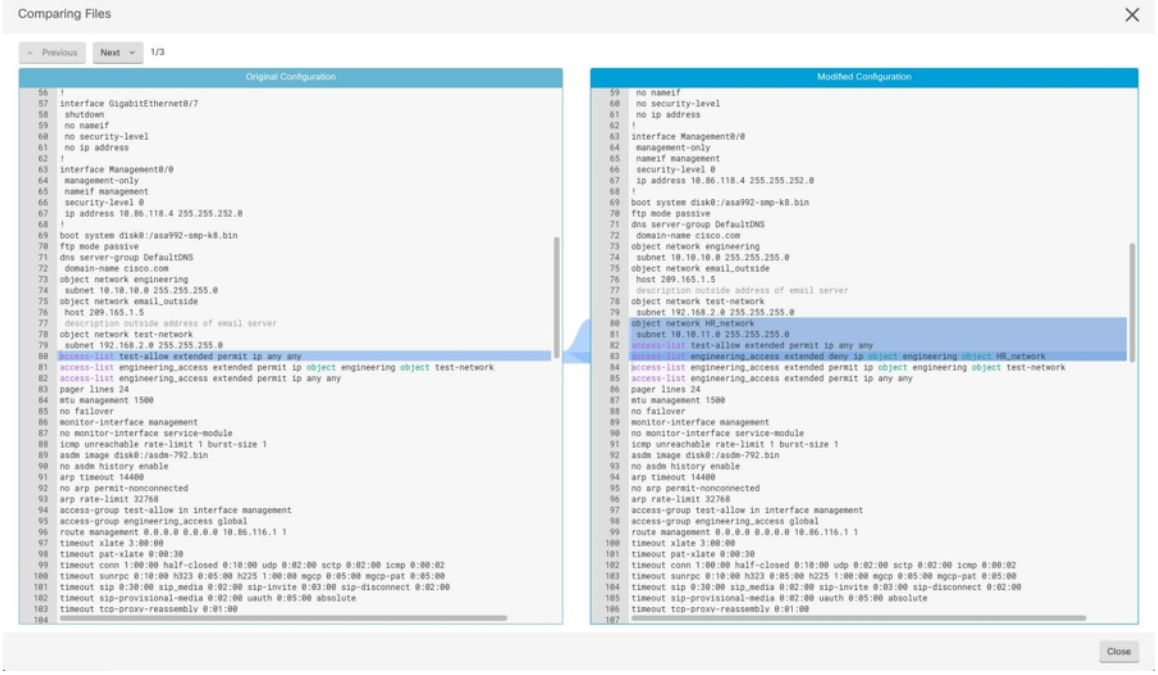
You can search and filter Change log entries. Use the search bar to find events that match your keywords.

Use the filter to find the entries that meet all the criteria you specify. You can also combine the operations by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

View Change Log Differences

Clicking the blue "Diff" link in the change log opens up a side-by-side comparison of the changes in the running configuration file of the device. You see the differences in the two versions.

In the illustration below, the "Original Configuration" is the running configuration file before a change was written to the ASA and 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 that actually didn'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 and you 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. Use the **Previous** and **Next** buttons to click through the changes in the file.



Related Topics

- Manage Change Logs in CDO, on page 133

Export the Change Log

You can export all or a subset of the CDO change log to a comma separated value (.csv) file so you can filter and sort the information in it however you like.

To export the change log to a .csv file, follow this procedure:

Step 1 In the navigation pane, click **Change Log**.

Step 2 Find the changes you want to export by taking one of these actions:

- Use the filter field and the search field to find exactly 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 Keep in mind, CDO stores 1 year of change log data. It may be better to filter the change log contents and download the results ot a .csv file rather than downloading up to a year of change log history.

Step 3 Click the blue export button in the top right of the change log .

Step 4 Give the .csv file a descriptive name and save the file to your local file system.

Differences Between the Change Log Capacity in CDO and the Size of an Exported Change Log

The information that you export from CDO's change log page is different from the change log information 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.

When you export the change log, however, 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 CDO stores.

CDO stores up to 1 year of change log information, this includes the two copies of the configuration.

Change Request Management

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

Note You may also see references to Change Request Tracking 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. To enable Change Request Tracking, follow this procedure:

Step 1 From the user menu, select Settings.

Step 2 From the user menu, click **General Settings**.

Step 3 Click the slider under "Change Request Tracking".

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

Create a Change Request

Step 1 On any page within CDO, click the +on the change request toolbar at the lower-left side of the page.

Step 2 Enter a change request name and description. The change request name must reflect a change request identifier your organization wants to implement. Use the description field to describe the purpose of change.

Note You can't change the name of a change request once you create it.

Step 3 Save the change request.

Note CDO saves the change request and associates all new changes with that change request name until you disable change requests or clear the change request information in the change request toolbar.

Associate a Change Request with a Change Log Event

Step 1 In the navigation pane, click **Change Log**.

Step 2 Expand the change log to show the events you want to associate with a change request.

Step 3 In the Change Request column, click the drop-down menu for the event. Note that the newest change requests are listed at the top of the change request list.

Step 4 Click the name of a change request and click **Select**.

Search for Change Log Events with Change Requests

Step 1 From the navigation pane, choose **Change Log**.

Step 2 In the Change Log search field, enter the exact name of the change request to find the change log events associated with that change request. CDO highlights change log events with exact matches.

Search for a Change Request

Step 1 Click the change request menu in the change request toolbar.

Step 2 Start entering the name of the change request or a relevant keyword in the search field. As you type, you see results that partially match your input, appearing in both the name and description fields within the list of change requests.

Filter Change Requests

Step 1 From the navigation pane, choose **Change Log**.

Step 2 Click the filter icon to expand it, start typing the change request name in the search field. As you type, results that partially match your entry begin to appear.

Step 3 Select the change request and check the corresponding check box. The matches appear in the **Change Log** table. CDO highlights change log events with exact matches.

Clear the Change Request Toolbar

Clear the change request toolbar to prevent change log events from being automatically associated with an existing change request.

Step 1 Select the change request menu in the change request toolbar.

Step 2 Click **Clear**. The change request menu changes to **None**.

Clear a Change Request Associated with a Change Log Event

Step 1 From the navigation pane, choose **Change Log**.

Step 2 Expand the change log to view the events that you want to disassociate from change requests.

Step 3 Click the change request drop-down list for the event.

Step 4 Click **Clear**.

Delete a Change Request

When you delete a change request, you delete it from the change request list not from the change log.

Step 1 Click the change request menu in the change request toolbar.

Step 2 Click the bin icon to delete a change request.

Step 3 Click the check mark to confirm.

Disable Change Request Management

Disabling change request management affects all users of your account. To disable Change Request Management, follow this procedure:

Step 1 From the navigation pane, choose **Settings**.

Step 2 Disable the **Change Request Tracking** toggle button.

Change Request Management Use Cases

These use cases assume that you have previously enabled Change Request Management following the above instructions.

Track Firewall Changes Made to Resolve a Ticket Maintained in an External System

In this use case, you are making firewall changes to resolve a ticket maintained in an external system. You want to associate change log events resulting from those firewall changes with a change request. Follow this procedure to create a change request and associate change log events with it.

1. Create a Change Request, on page 137. 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 or other relevant information.
2. Ensure that the new change request is visible in the change request toolbar.
3. Make the firewall changes.
4. In the navigation pane, choose **Change Log** and find change log events that are associated with your new change request.
5. Clear the Change Request Toolbar, on page 138 when done.

Manually Update Individual Change Log Events After Firewall Changes Are Made

In this use case, you made firewall changes 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 137. 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 or other relevant information.
2. In the navigation pane, choose **Change Log** and search for the change log events that are associated with the firewall changes.
3. Associate a Change Request with a Change Log Event, on page 137.
4. Clear the Change Request Toolbar, on page 138 when done.

Search for Change Log Events Associated with a Change Request

In this use case, your requirement is to find out what change log events were recorded in the Change Log due to the work that is 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, choose **Change Log.**
2. Search for change log events that are associated with change requests using one of these methods.
   - 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 with exact matches.
   - Filter Change Requests, on page 138 to find the change log events.
3. View each change log to find the highlighted change log events showing the associated change request.

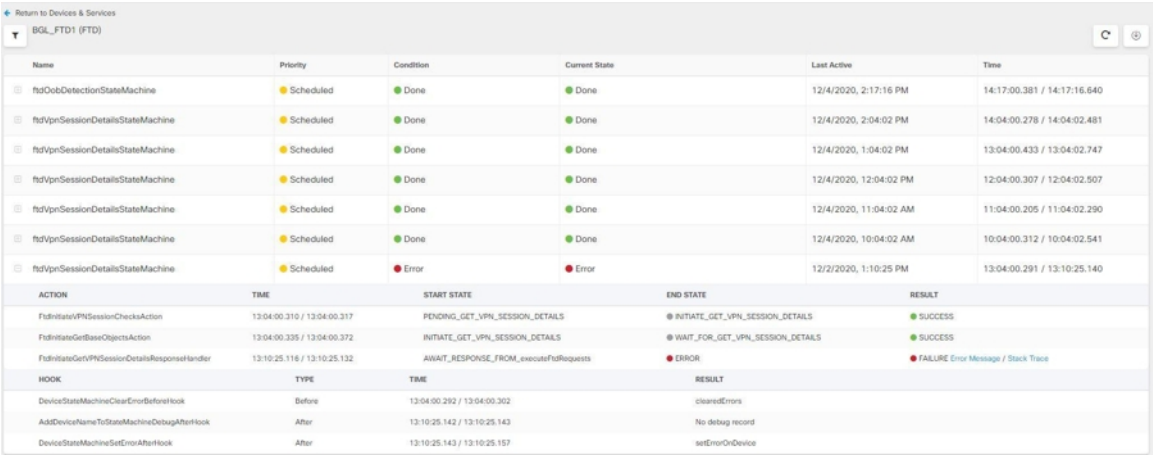
Monitor Workflows in CDO

The Workflow 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, and you can navigate to the Workflows page to see the step where the error occurred for more details.

You can visit this page to determine and troubleshoot errors or share information with TAC when they insist.

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. In the **Devices and Actions** in the right pane, click **Workflows**. The following picture shows the Workflow page with entries in the Workflow table.

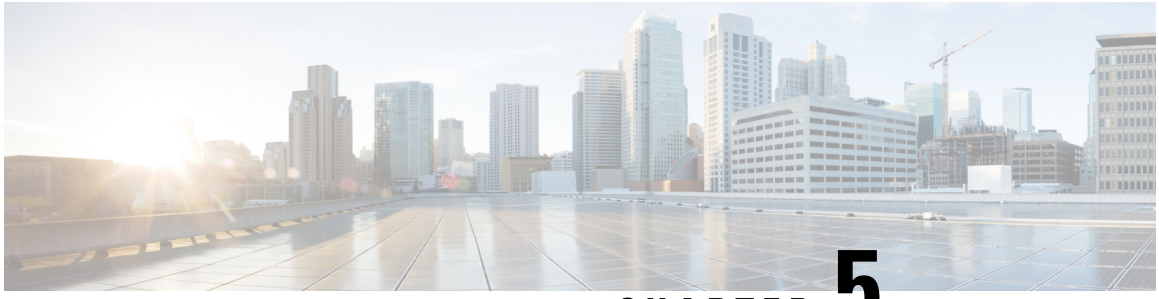


Export Device Workflows

You can download the complete workflow information to a JSON file and provide it when the TAC team asks for further analysis. To export this information, you can select the device and navigate to its Workflows page and click the export button appearing on the top right corner.

Copy Stack Trace

If you have an error you cannot resolve, TAC may ask you for a copy of the stack trace. To collect the stack trace for the error, click the **Stack Trace** link and click **Copy Stacktrace** to copy the stacks appearing on the screen to a clipboard.



CHAPTER 5

Integrating CDO with Cisco Security Cloud Sign On

- SecureX and CDO, on page 143

SecureX and CDO

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and the customer's infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications. By connecting technology in an integrated platform, SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. For more about what SecureX is and what this platform offers, see About SecureX.

Allowing SecureX to access your CDO tenant results in a summarization of device events, including a total count of device as well as a count of devices with errors, devices with conflicts, and devices that may currently be out-of-sync. The summary of events also provides a second window that tallies currently applied policies and the objects associated to those policies. Policies are defined by device-type, and objects are identified via object type.

Multiple steps are required to add a CDO module to the SecureX dashboard. See Add CDO to SecureX for more information.

Warning If you have not already merged your CDO and SecureX accounts, you may not be able to see the events for all of your onboarded devices. We **strongly** recommend merging your accounts before you create a CDO module inSecureX. See Merge Your CDO and SecureX or Cisco XDR Tenant Accounts for more information.

Related Information:

- About SecureX
- Merge Your CDO and SecureX or Cisco XDR Tenant Accounts
- Add CDO to SecureX

Merge Your CDO and SecureX or 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 SecureX or Cisco XDR, you must link your CDO tenant account with the SecureX or 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.

Add CDO to SecureX

Allow SecureX to access your registered devices and add the CDO module to the SecureX dashboard to see a summary of your device policies and objects alongside the other Cisco platforms in your security portfolio.

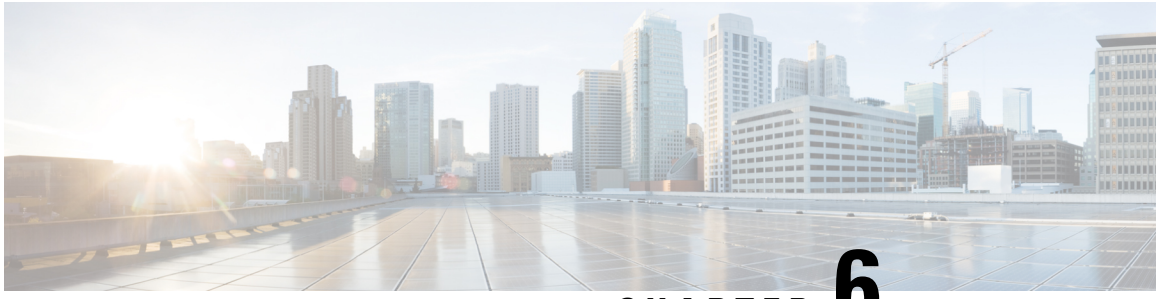
Note Be mindful of when you initiatie this process. Merging CDO to SecureX may take an extended amount of time.

Before you begin

We strongly recommend the following action items before connecting SecureX in CDO:

- You must be at least an Administrator for your SecureX account.
- You must have a SuperAdmin user role for your CDO tenant.
- Merge your tenant accounts in Security Services Exchange to facilitate tenant communication. See Merge Your CDO and SecureX or Cisco XDR Tenant Accounts for more information.
- After merging your CDO tenant with Security Services Exchange, ensure that you log out of your CDO tenant and log in again.
- If you have not already done so, configure Cisco Secure Sign-On as your SAML single sign-on identity provider (IdP) and Duo Security for multi-factor authentication (MFA). Both CDO and SecureX use this as an authentication method. See Integrate Your SAML Single Sign-On with Cisco Defense Orchestrator for more information.

Note **Note**: If you have multiple tenants, you must create one module per tenant in SecureX. Each tenant requires a unique API token for authorization.



CHAPTER 6

Terraform

- About Terraform, on page 145

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:

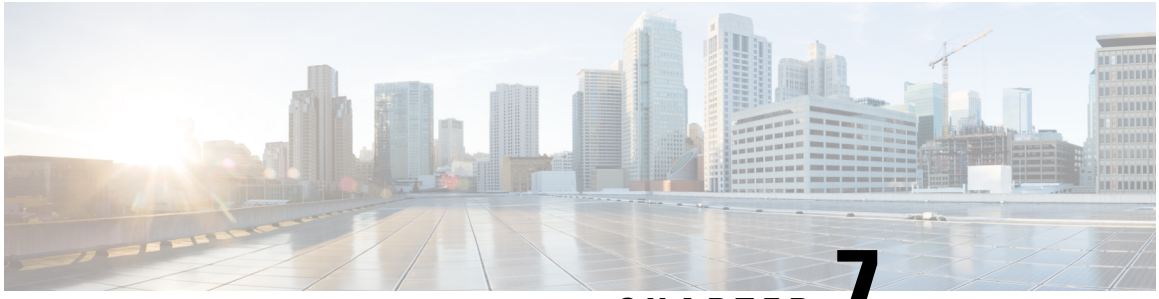
Module	Repository
CDO Terraform Provider	https://github.com/ciscodevnet/terraform-provider-cdo
CDO SDC Module (vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-cdo-sdc
CDO SDC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-cdo-sdc
CDO SEC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-cdo-sec

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 7

Troubleshooting

This chapter covers the following sections:

- Troubleshoot a Secure Device Connector, on page 147
- Troubleshoot Cisco Defense Orchestrator, on page 154
- Device Connectivity States, on page 162

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 Cisco Defense Orchestrator 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. From the CDO menu, 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 Does not Become Active on CDO after Deployment, on page 148.

.

SDC Status Does not Become 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 `[cdo@localhost cdo]$` 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 Cisco Defense Orchestrator 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 From the CDO menu, choose **Tools & Services** > **Secure Connectors**.

Step 2 Select the SDC.

Step 3 In the **Troubleshooting** pane on the right, click **Device Connectivity**.

Step 4 Enter a valid IP address or FQDN and port number of the device you are attempting to troubleshoot, or attempting to connect to, and click **Go**. 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 5 If you continue to have issues onboarding or connecting to the device, Contact Cisco Defense Orchestrator 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 150
  - Updating a Custom SDC Host, on page 151
  - Bug Tracking, on page 151

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 (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 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

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 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 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.

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. Click the **CDO** tile to access defenseorchestrator.com or **CDO (EU)** to access defenseorchestrator.eu.

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 59.

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 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 account, click the CDO tile on the dashboard that corresponds to Cisco Defense Orchestrator(US), Cisco Defense Orchestrator (EU), or Cisco Defense Orchestrator (APJC)
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Access and Certificates

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 In the navigation pane, choose **Analytics** > **Event Logging** .

Step 2 Click the **Historical** tab.

Step 3 Start filtering events by **Time Range**. By default, the Historical tab shows the last hour of events. If that is the correct time range, enter the current date and time as the **End** time. If that is not the correct time range, enter a start and end time encompassing the time of the reported issue.

Step 4 Enter the IP address of the firewall that you suspect is controlling the user's access in the **Sensor ID** field. If it could be more than one firewall, filter events using **attribute:value** pairs in the search bar. Make two entries and combine them with an OR statement. For example: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

Step 5 Enter the user's IP address in the **Source IP** field in the Events filter bar.

Step 6 If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.

Step 7 Expand the events in the results and look at their details. Here are some details to look at:

- **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.
- **FirewallPolicy** - The policy in which the rule that triggered the event resides.
- **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.
- **UserName** - The user associated with the initiator IP address. The Initiator IP address is the same as the Source IP address.

Step 8 If the rule action is preventing access, look at the FirewallRule and FirewallPolicy fields to identify the rule in the policy that is blocking access.

Troubleshooting SSL Decryption Issues

Handling Web Sites Where Decrypt Re-sign Works for a Browser but not an App (SSL or Certificate Authority Pinning)

Some apps for smart phones and other devices use a technique called SSL (or Certificate Authority) pinning. The SSL pinning technique embeds the hash of the original server certificate inside the app itself. As a result, when the app receives the resigned certificate from the Firepower Threat Defense device, the hash validation fails and the connection is aborted.

The primary symptom is that users cannot connect to the web site using the site's app, but they can connect using the web browser, even when using the browser on the same device where the app fails. For example, users cannot use the Facebook iOS or Android app, but they can point Safari or Chrome at https://www.facebook.com and make a successful connection.

Because SSL pinning is specifically used to avoid man-in-the-middle attacks, there is no workaround. You must choose between the following options:

More Details

If a site works in a browser but not in an app on the same device, you are almost certainly looking at an instance of SSL pinning. However, if you want to delve deeper, you can use connection events to identify SSL pinning in addition to the browser test.

There are two ways an app might deal with hash validation failures:

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the server. The Alert is usually an "Unknown CA (48)" alert indicating SSL Pinning. A TCP Reset is sent following the Alert message. You should see the following symptoms in the event details:
  - `SSL Flow Flags include ALERT_SEEN.`
  - `SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.`
  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.`
- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is done and then send a TCP Reset. You should see the following symptoms in the event:
  - `SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.`
  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.`

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 59.

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 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 account, click the CDO tile on the dashboard that corresponds to Cisco Defense Orchestrator(US), Cisco Defense Orchestrator (EU), or Cisco Defense Orchestrator (APJC)
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Objects

Resolve Duplicate Object Issues

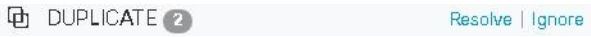
Duplicate objects are two or more objects on the same device with different names but the same values. These objects are usually created accidentally, serve similar purposes, and are used by different policies. After resolving duplicate object issues, CDO updates all affected object references with the retained object name.

To resolve duplicate object issues:

Step 1 In the CDO navigation bar on the left, 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 74
- Bulk Reconnect Devices to CDO, on page 78

Resolve an Unused Object Issue

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 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 122 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 CDO navigation bar on the left, 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.

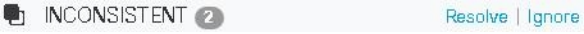
Step 4 In the Actions pane on the right, click **Remove** to remove all the unused objects you selected in CDO. You can remove 99 objects at a time.

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 160 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.

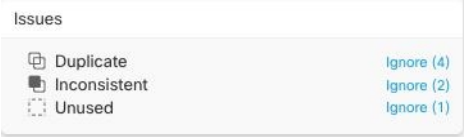
Important If the object becomes associated with another issue type at a later time, the ignore action you committed only affects the issues you selected at that time. For example, if you ignored an object because it was a duplicate and the object is later marked inconsistent, ignoring it as a duplicate object does not mean it will be ignored as an inconsistent object.

To ignore issues in bulk, follow this procedure:

Step 1 In the CDO navigation bar on the left, 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.

Device Connectivity State	Possible Reasons	Resolution
Insufficient licenses	Device doesn't have sufficient licenses.	Troubleshoot Insufficient Licenses, on page 163
Invalid credentials	Username and password combination used by CDO to connect to the device is incorrect.	Troubleshoot Invalid Credentials, on page 164
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 164
Onboarding Error	CDO may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error, on page 172

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 CDO navigation bar, 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 Open the **Inventory** page.

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 126 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.

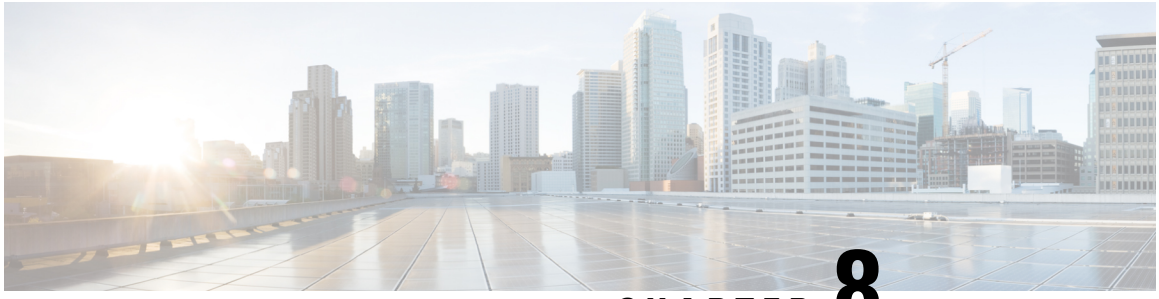
Step 3 Click the appropriate device type tab.

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 8

FAQ and Support

This chapter contains the following sections:

- Cisco Defense Orchestrator, on page 175
- FAQ About Onboarding Devices to Cisco Defense Orchestrator, on page 176
- Device Types, on page 177
- Security, on page 179
- Troubleshooting, on page 180
- Terminologies and Definitions used in Low-Touch Provisioning, on page 180
- Policy Optimization, on page 181
- Connectivity, on page 181
- About Data Interfaces, on page 182
- How CDO Processes Personal Information, on page 182
- Contact Cisco Defense Orchestrator Support, on page 182

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 low-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 122

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 requre 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 Low-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.
- **Low-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.

- **Serial number onboarding** - It is the process of onboarding an FTD using its serial number that has already been configured (installed and setup).

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.

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 73) and then reconnect the device (see Bulk Reconnect Devices to CDO, on page 78). 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 Cisco Defense Orchestrator 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).

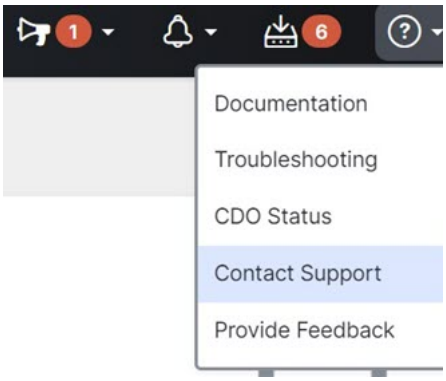
- How CDO Customers Open a Support Ticket with TAC.
- How CDO Trial Customers Open a Support Ticket with TAC.

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.

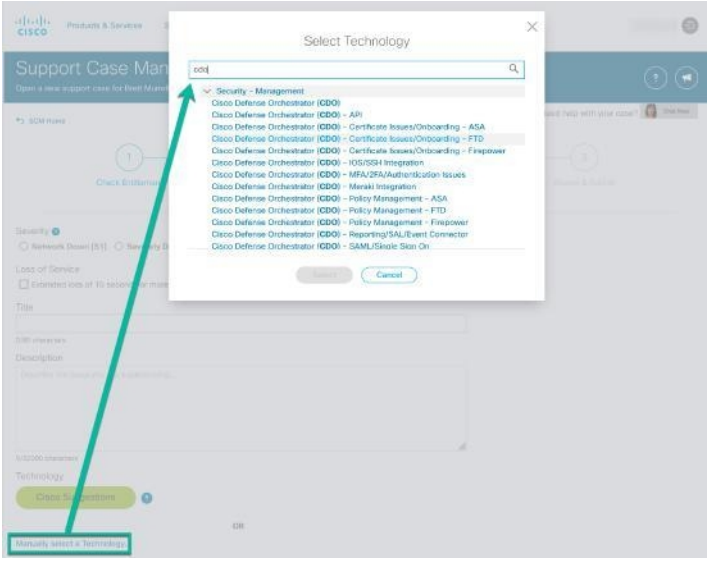
- **Important**: In order for your case to be associated with your Cisco.com account, you need to associate your contract number to your Cisco.com profile. Use this procedure to associate your contract number to your Cisco.com profile.
  a. Open to Cisco Profile Manager.
  b. Click the **Access Management** 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**.



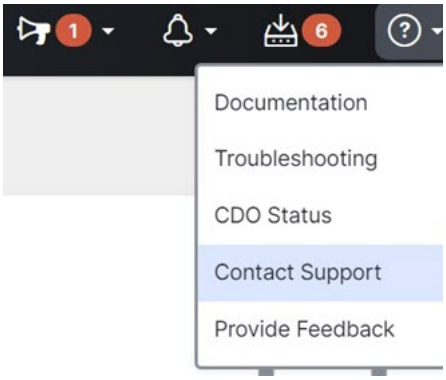
Step 13 Complete the remainder of the service request and click **Submit**.

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.