# Basics of CDO

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


- Create a CDO Tenant, 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 6
- Manage Super Admins on Your Tenant, on page 7
- About CDO Licenses, on page 7
- Secure Device Connector, on page 9
- Devices, Software, and Hardware Supported by CDO, on page 38
- Browsers Supported in CDO, on page 40
- **CDO Platform Maintenance Schedule**, on page 40
- Cloud-delivered Firewall Management Center Maintenance Schedule, on page 41
- Manage a CDO Tenant, on page 41
- Manage Users in CDO, on page 59
- Active Directory Groups in User Management, on page 60
- Create a New CDO User, on page 66
- User Roles in CDO, on page 71
- Add a User Account to CDO, on page 75
- Edit a User Record for a User Role, on page 76
- Delete a User Record for a User Role, on page 77
- CDO Services Page, on page 77
- CDO Device and Service Management, on page 80
- CDO Inventory Information, on page 88
- CDO Labels and Filtering, on page 88
- Use CDO Search Functionality, on page 90
- Objects, on page 91


# Create a CDO Tenant

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

### Procedure

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

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

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

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

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

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

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

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

### Upgrade your CDO tenant to full version

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

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

### Request CDO trial period extension

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

# Sign in to CDO

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

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

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

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

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

**Note**

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

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

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

# Initial Login to Your New CDO Tenant

### Before You Begin

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

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

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

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

**Important** **If your CDO tenant existed before October 14, 2019**, use Migrate to Cisco Security Cloud Sign On Identity Provider, on page 4 for log in instructions instead of this article.

### What to do next?

Continue to, Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication, on page 67. It is a four-step process. You need to complete all four steps.

## Signing in to CDO in Different Regions

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

***Table 1: CDO URLs in Different Regions***

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

## Troubleshooting Login Failures

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

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

See Signing in to CDO in Different Regions, on page 4 for information about which region you shoud sign into.

# Migrate to Cisco Security Cloud Sign On Identity Provider

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

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

**Note**

- If you sign in to CDO using your own single sign-on identity provider, this transition to Cisco Security Cloud Sign On and Duo does not affect you. You continue to use your own sign-on solution.
- If you are in the middle of a free trial of CDO, this transition does apply to you.
- **If your CDO tenant was created on or after October 14, 2019**, see Initial Login to Your New CDO Tenant, on page 3 for log in instructions instead of this article.

### Before You Begin

We strongly recommend the following steps prior to migrating:

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

# Troubleshooting Login Failures after Migration

### Login to CDO Fails Because of Incorrect Username or Password

**Solution** If you try to log in to CDO and you *know* you are using the correct username and password and your login is failing, or you try "forgot password" cannot recover a viable password, you may have tried to login without creating a new Cisco Security Cloud Sign On account, you need to sign up for a new Cisco Security Cloud Sign On Account by following the instructions in Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication, on page 67.

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

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

### Login Fails Using a Saved Bookmark

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

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

- **Solution** If you have not yet created a Cisco Secure Sign-On account, Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication.
- **Solution** If you have created your new secure sign-on account, click the CDO tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Cisco Defense Orchestrator APJ

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

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

# Launch a CDO Tenant

**Procedure**

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

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

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

The **Portals** view retrieves and displays consolidated information from multiple tenants. See Manage Multi-Tenant Portal, on page 55 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 CDO to your Managed Devices, on page 10 for information explaining how to allow communication between between an SDC and CDO.

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

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

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

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

The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC. The initial SDC on your tenant incorporates the name of your tenant and the number 1 and is displayed on the **Secure Connectors** tab in the **Services** page of CDO. Each additional SDC is numbered in order. See Deploy a Secure Device Connector Using CDO's VM Image, on page 11 and Deploy a Secure Device Connector On Your VM, on page 15

**Related Information:**

- Connect CDO to your Managed Devices
- Update your Secure Device Connector, on page 28
- Remove a Secure Device Connector, on page 26

# Connect CDO to your Managed Devices

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

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

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

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

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

- A device with SSH access.

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

### Connecting Devices to CDO Through the Cloud Connector

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

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

- 54.199.195.111
- 52.199.243.0

If you are a customer in the **Australia (AUS)** region, and you connect to CDO at https://aus.cdo.cisco.com, allow inbound access from the following IP addresses:

- 13.55.73.159
- 13.238.226.118

If you are a customer in **Europe, the Middle East, or Africa (EMEA)** region, and you connect to CDO at https://defenseorchestrator.eu/, allow inbound access from the following IP addresses:

- 35.157.12.126
- 35.157.12.15

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

- 35.154.115.175
- 13.201.213.99

If you are a customer in the **United States (US)** region, and you connect to CDO at https://defenseorchestrator.com, allow inbound access from the following IP addresses:

- 52.34.234.2
- 52.36.70.147

### Connecting CDO to SDC

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

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

# 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 28 for more information.

This procedure describes how to install an SDC in your network, using CDO's VM image. This is the preferred, easiest, and most reliable way to create an SDC. If you need to create the SDC using a VM that you create, follow Deploy a Secure Device Connector On Your VM, on page 15.

### Before you begin

Review these prerequisites before you deploy the SDC:

- CDO requires strict certificate checking and does not support Web/Content Proxy inspection between the Secure Device Connector (SDC) and the Internet. If using a proxy server, disable inspection for traffic between the SDC and CDO.
- The SDC must have full outbound access to the internet on TCP port 443, or the port you have configured for device management. The devices managed by CDO must also allow inbound traffic from this port.
- Review Connect CDO to your Managed Devices to ensure proper network access.
- CDO supports installing its SDC VM OVF image using the vSphere web client or the ESXi web client.
- CDO does not support installing the SDC VM OVF image using the vSphere desktop client.
- ESXi 5.1 hypervisor.
- Cent OS 7 guest operating system.
- System requirements for a VMware ESXi host with only one SDC:

    - VMware ESXi host needs 2 CPU.
    - VMware ESXi host needs a minimum of 2 GB of memory.
    - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice.
- The dockers IP must be in a different subnet than the SDC's IP range **and** the device IP range.
- Gather this information before you begin the installation:
    - Static IP address you want to use for your SDC.
    - Passwords for the `root` and `cdo` users that you create during the installation process.
    - The IP address of the DNS server your organization uses.
    - The gateway IP address of the network the SDC address is on.
    - The FQDN or IP address of your time server.
- The SDC virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

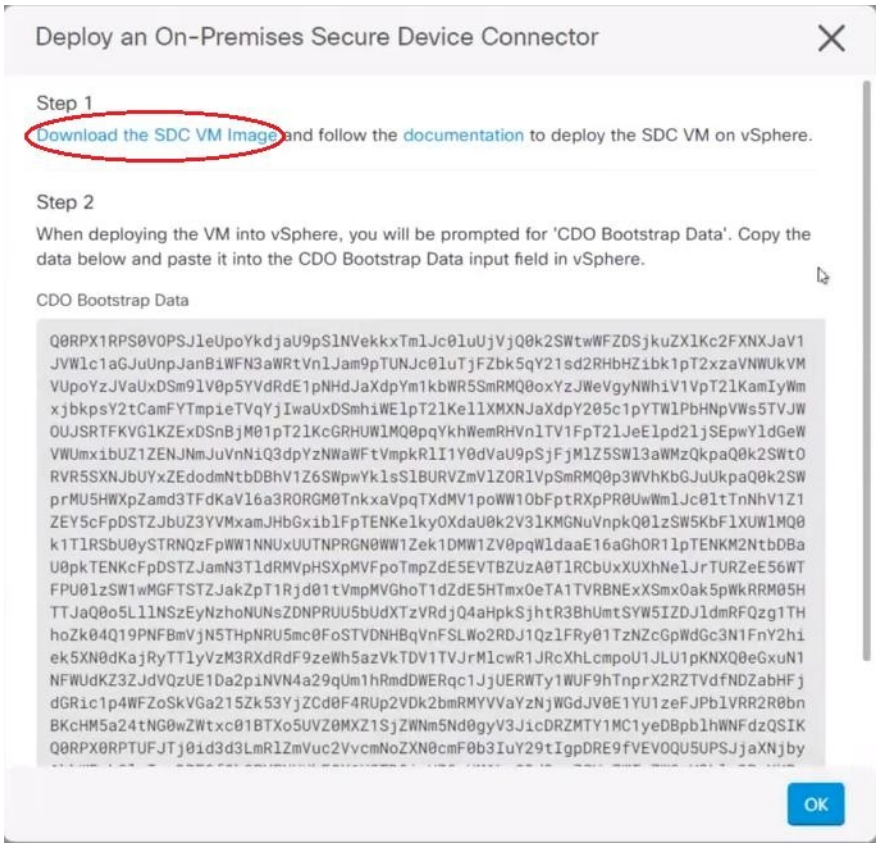
### Procedure

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

**Step 2** From the CDO menu, choose **Tools & Services** > **Secure Connectors**.

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

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




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

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

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

**Note** Do not use the ESXi Web Client.

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

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

**Step 9** Open the console for your new SDC VM.

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

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

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

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

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

**Step 14** Follow the prompts to create a new password for the CDO user. Enter your password for the user

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

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

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

or press enter if a docker bridge is not applicable.

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

**Step 18** Confirm your entries.

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

**Step 20** The VM console automatically logs you out.

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

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

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

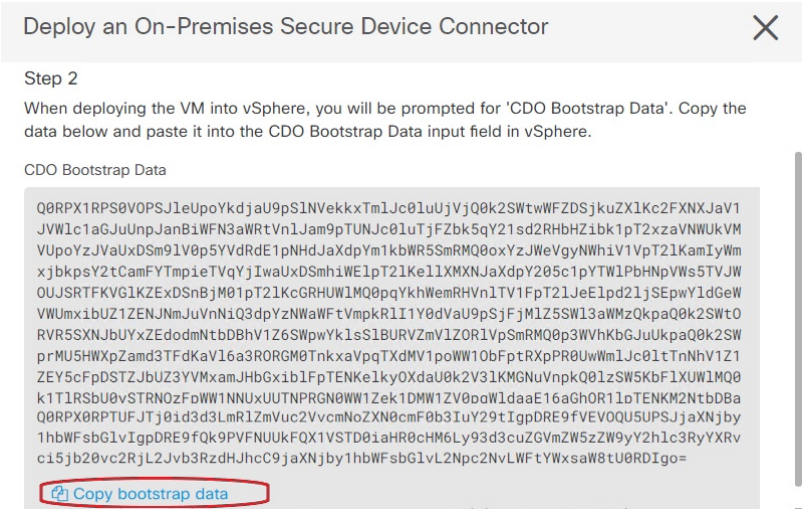
**Step 23** When prompted with **[sudo] password**, enter the password you created in Step 14.

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

**a.** Log into CDO.

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

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




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

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

# Deploy a Secure Device Connector On Your VM

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

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

The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices. See Using Multiple SDCs on a Single CDO Tenant, on page 28 for more information.

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

**Note** The preferred, easiest, and most reliable way to install an SDC is to download CDO's SDC OVA image and install it. See Deploy a Secure Device Connector Using CDO's VM Image, on page 11 for those instructions.

### Before you begin

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

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

- ESXi 5.1 hypervisor.
- Cent OS 7 guest operating system.
- System requirements for a VM with only an SDC:
  - VMware ESXi host needs 2 CPUs.
  - VMware ESXi host needs a minimum of 2 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice. This value assumes you are using Logical Volume Management (LVM) with the partition so you can expand required disk space as needed.

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

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

### Procedure

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

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

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

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

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

- 8GB of RAM
- 10GB disk space

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

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

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

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

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

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

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

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

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

**Note** Use the "Install using the repository" method.

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

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

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

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

**Step 15** Set a password for the CDO user.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Step 24** Download the bootstrap bundle from CDO.

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

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

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/CDO/tenant-name-SDC
               <snipped - extracted files>
               [sdc@sdc-vm ~]$
               [sdc@sdc-vm ~]$ /usr/local/ CDO/bootstrap/bootstrap.sh
               [2018-07-23 13:54:02] environment properly configured
               download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
               toolkit.sh
               common.sh
               [2018-07-23 13:54:04] startup new container
               Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
               sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
               ciscodefenseorchestrator/sdc_prod
               08d48e6f1cff: Pull complete
               ebbd10b629b1: Pull complete
               d14d580ef2ed: Pull complete
               45421d451ab8: Pull complete
               <snipped - downloads>
               no crontab for sdc
```

The SDC should now show "Active" in CDO.

---

### What to do next

-

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

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

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

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

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

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

### Before you begin

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

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

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

  SDC:

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

  SDC and SEC:

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

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

### Procedure

**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

### Procedure

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

**Step 2** Configure the CDO Terraform provider in your Terraform repository by following the instructions in CDO Terraform Provider.

**Example:**

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

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

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

**Example:**

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

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

**Step 4** Write Terraform code to create the SDC in vSphere using CDO_sdc Terraform module.

**Example:**

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

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

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

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

See the CDO Automation Repository in the CiscoDevNet for a complete example.

---

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

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

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

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

### Before you begin

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

- CDO requires strict certificate checking and does not support Web/Content Proxy inspection between the SDC and the Internet. If using a proxy server, disable inspection for traffic between the Secure Device Connector (SDC) andCDO.
- Review Connect CDO to your Managed Devices to ensure proper network access.

- You require an AWS account, an AWS VPC with at least one subnet, and an AWS Route53-hosted zone.
- Ensure you have the CDO bootstrap data, your AWS VPC ID, and its subnet ID handy.
- Ensure that the private subnet to which you deploy the SDC has a NAT gateway attached.
- Open traffic on the port on which your firewall management HTTP interface is running, from your firewalls to the Elastic IP attached to the NAT gateway.

### Procedure

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

```
module "example-sdc" {
  source              =
"git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env                 = "example-env-ci"
  instance_name       = "example-instance-name"
  instance_size       = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id              = <replace-with-vpc-id>
  subnet_id           = <replace-with-private-subnet-id>
}
```

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

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

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

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

### What to do next

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

**Note** The 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.

### Procedure

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

```
$ sudo su - sdc
```

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

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

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

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

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

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

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

b) Restart the container using this command:

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

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

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

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

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

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

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

# Change the IP Address of a Secure Device Connector

### Before you begin

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

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

### Procedure

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

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

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

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

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

**Step 4** Enter your password at the prompt.

```
[sudo] password for cdo:
```

**Step 5** Type `n` at the prompt for resetting the root and CDO passwords.

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

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

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

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

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

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

e) Docker Bridge

   or press enter if a docker bridge is not applicable.

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

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

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

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

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

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

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

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

**Step 11** You can also check your SDC's connectivity through the CDO user interface. To do that, open the CDO application and navigate to **Tools & Services** > **Secure Connectors** page.

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

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

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

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

See Deploy a Secure Device Connector On Your VM, on page 15 for information on deploying an SDC on your VM.

# Remove a Secure Device Connector

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

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

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

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

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

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

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

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

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

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

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

# Move an ASA from one SDC to Another

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

**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

**Procedure**

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

**Step 2** Select the SDC you want to rename.

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

**Step 4** Rename the SDC.

This new name will appear wherever the SDC name appears in the 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.

### Procedure

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

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

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

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

**Step 4** Upgrade the SDC toolkit:

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

**Step 5** Upgrade the SDC:

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

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

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

# Using Multiple SDCs on a Single CDO Tenant

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

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

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

# CDO Devices that Use the Same SDC

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

**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.

**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

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

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

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

**Note**

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

# Cloud-delivered Firewall Management Center Maintenance Schedule

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

**Note**

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

# Manage a CDO Tenant

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

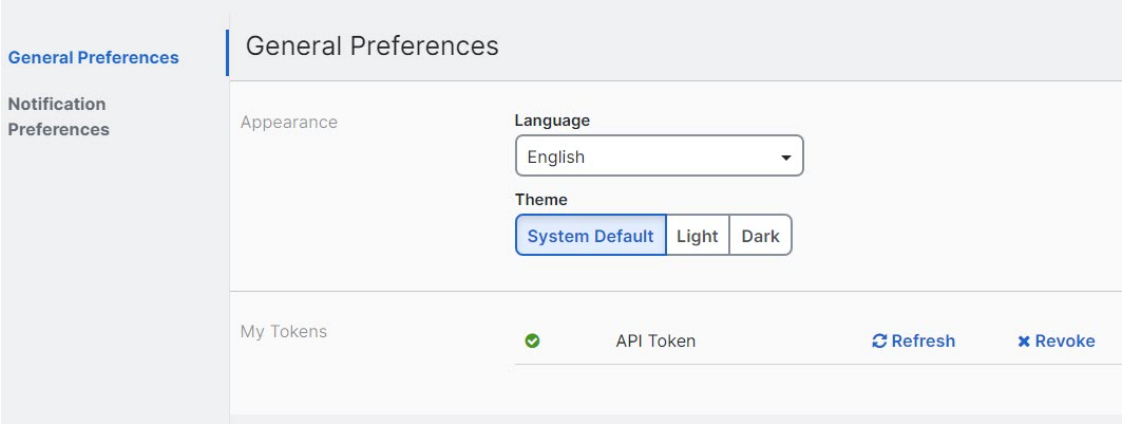
## General Settings

See the following topics regarding general CDO Settings:

- General Preferences, on page 42
- For **My Tokens**, see API Tokens, on page 52
- For **Tenant Settings**, see:
  - Enable Change Request Tracking, on page 42
  - Prevent Cisco Support from Viewing your Tenant, on page 43
  - Enable the Option to Auto-accept Device Changes, on page 43
  - Default Conflict Detection Interval, on page 43
  - Web Analytics, on page 44
  - Tenant ID, on page 44
  - Tenant Name, on page 45

# General Preferences

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




# Change the CDO Web Interface Appearance

You can change the way the web interface appears.

**Procedure**

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

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

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

# My Tokens

See API Tokens for more information.

# Tenant Settings

## Enable Change Request Tracking

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

**Procedure**

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

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

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

### Prevent Cisco Support from Viewing your Tenant

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

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

**Procedure**

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

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

### Enable the Option to Auto-accept Device Changes

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

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

**Procedure**

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

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

### Default Conflict Detection Interval

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

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

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

**Procedure**

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

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

## Enable the Option to Schedule Automatic Deployments

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

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

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

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

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

### Procedure

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

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

## Web Analytics

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

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

### Procedure

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

**Step 2** In the Tenant Settings area, click the slider under **Web Analytics**.

## Tenant ID

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

### Tenant Name

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

# View CDO Notifications

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

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

### Overview Tab

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

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

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

### All Tab

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

### Dismissed Tab

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

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

### Search Notifications

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

# User Notification Preferences

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

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

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

### Send Alerts for Device Workflows

- **Deployments** - This action does not include integration instances for SSH or IOS devices.
- **Backups** - This action is only applicable for FDM-managed devices.
- **Upgrades** - This action is only applicable for ASA and FDM-managed devices.
- **Migrate FTD to cloud** - This action is applicable when changing the FTD device manager from FMC to CDO.

### Send Alerts for Device Events

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

### Send Alerts for Background Log Search

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

### Opt Out of Notification Preferences

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

### Email Alerts

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

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

# Tenant Notification Settings

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

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

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

### Email Subscribers

Add or modify the emails that receive alerts from your CDO tenant. See Enable Email Subscribers, on page 47 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 Change Log 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.

### Procedure

**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.

### Procedure

**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.

### Procedure

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

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

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

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

## Enable Service Integrations for CDO Notifications

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

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

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

### Incoming Webhooks for Webex Teams

#### Before you begin

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

- A Webex account.
- A CDO account and tenant.

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

#### Procedure

**Step 1** Open the Webex apphub.

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

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

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

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

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

**Step 5** Copy the Webhook URL.

**Step 6** Log into CDO.

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

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

**Step 9** Scroll to **Service Integrations**.

**Step 10** Click the blue plus button.

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

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

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

**Step 14** Click **OK**.

## Incoming Webhooks for Slack

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

Use the following procedure to allow incoming webhooks for Slack:

### Procedure

**Step 1** Log into your Slack account.

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

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

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

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

**Step 6** Use the drop-down menu to select the Slack channel you want the 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:

#### Procedure

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

**Step 2** Log into CDO.

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

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

**Step 5** Scroll to **Service Integrations**.

**Step 6** Click the blue plus button.

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

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

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

**Step 10** Click OK.

## Logging Settings

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

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

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

# Integrate Your SAML Single Sign-On with

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

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

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

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

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

# Renew SSO Certificate

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

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

(legacy only) If your Identity Provider (IdP) integration is directly with CDO, open a support ticket with CDO 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

**Procedure**

**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.

**Procedure**

**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

**Procedure**

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

**Step 2** In My Tokens, click **Revoke**. CDO revokes the token.

# Relationship Between the Identity Provider Accounts and CDO User Records

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

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

## Login Workflow

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

### Procedure

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

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

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

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

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

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

## Implications of this Architecture

### Customers Who Use Cisco Security Cloud Sign On

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

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

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

### Customers Who Have Their Own Identity Provider

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

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

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

### Cisco Managed Service Providers

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

### Related Topics

- General Settings
- Manage Users in CDO
- User Roles in CDO

# Manage Multi-Tenant Portal

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

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

### Before you begin

The multi-tenant portal is only available if the feature is enabled on your tenant. To enable multi-tenant portal for your tenant, open a support ticket with Cisco TAC. Once the support ticket is resolved and the portal is created, users with the **Super Admin** role on the portal have the ability to add tenants to it.

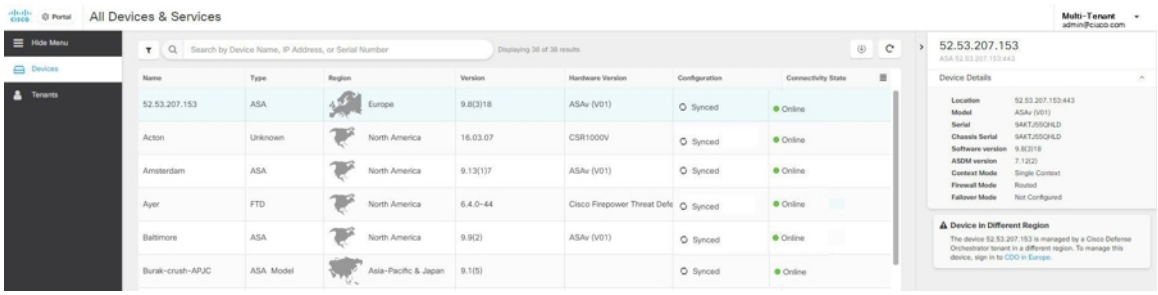
We recommend you clearing cache and cookies from your web browser to avoid certain browser-related issues that may occur.

### The Multi-Tenant Portal

The portal provides the following menus:

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

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




- **Tenants**:

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

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

- Create a CDO tenant
- Add an existing CDO tenant to the multitenant portal

## Add a Tenant to a Multi-Tenant Portal

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

**Important** We recommend that you Create API Only Users for your tenant and generate an API token for authenticating to CDO.

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

**Procedure**

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

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

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

**Step 4** Click add the tenant button on the right.

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

## Delete a Tenant from a Multi-Tenant Portal

**Procedure**

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

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

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

## Manage-Tenant Portal Settings

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

### Settings

#### General Settings

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

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

1. From the CDO dashboard, click **Settings** in the navigation bar to the left.
2. Click **General Settings**.
3. Click the slider under **Web Analytics**.

#### User Management

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

### Switch Tenant

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

#### Procedure

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

**Step 2** Click **Switch tenant**.

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

# The Cisco Success Network

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

- To inform you of available unused features that can improve the effectiveness of the product in your network.

- To inform you of additional technical support services and monitoring that might be available for your product.
- To help Cisco improve our products.

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

**Note**

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

### Enable or Disable the Cisco Success Network

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

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

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

# Manage Users in CDO

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

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

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

## View the User Records Associated with your Tenant

### Procedure

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

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

# Active Directory Groups in User Management

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

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

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

### Active Directory Groups Tab

In the left pane, choose **Settings** > **User Management** > **Active Directory Groups**. This page shows the Active Directory groups that are currently mapped to CDO. Most importantly, this page displays the role of the Active Directory group as assigned in your Active Directory manager.

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

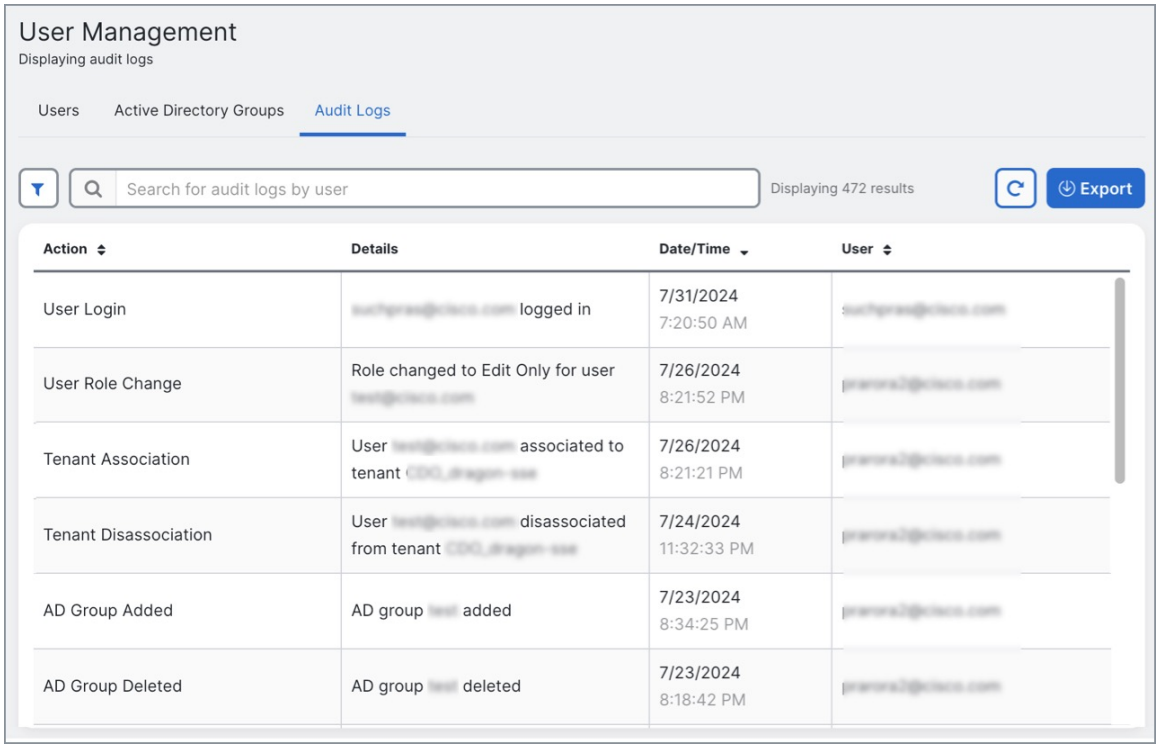
### Audit Logs

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

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

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

*Figure 1: Audit Logs*




### Multi-role Users

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

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

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

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

### API Endpoints for Active Directory Groups

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

- Create an Active Directory group
- Remove an Active Directory group

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

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

# Prerequisites for Adding an Active Directory Group to CDO

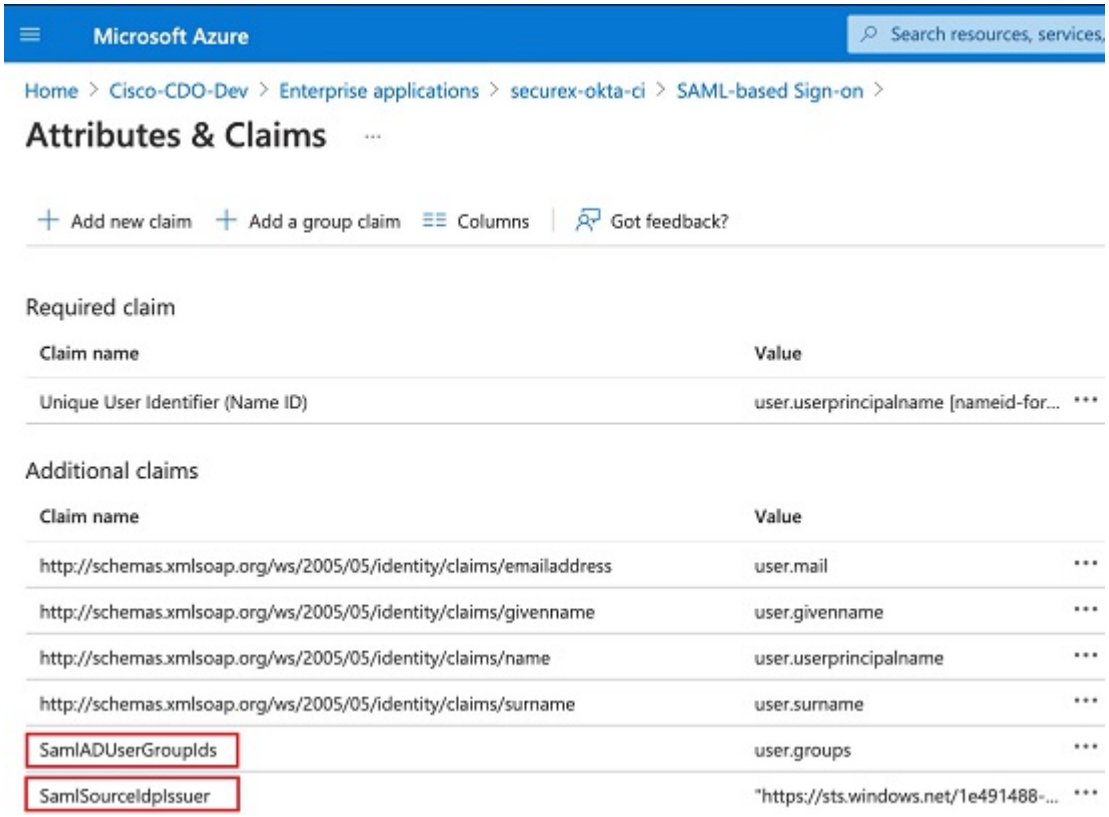
Before adding an Active Directory group mapping to CDO as a form of user management, you must have your Active Directory that is integrated with Security Cloud Sign On. If your Active Directory Identity Provider (IdP) is not already integrated, see identity provider integration guide to integrate a custom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

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

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

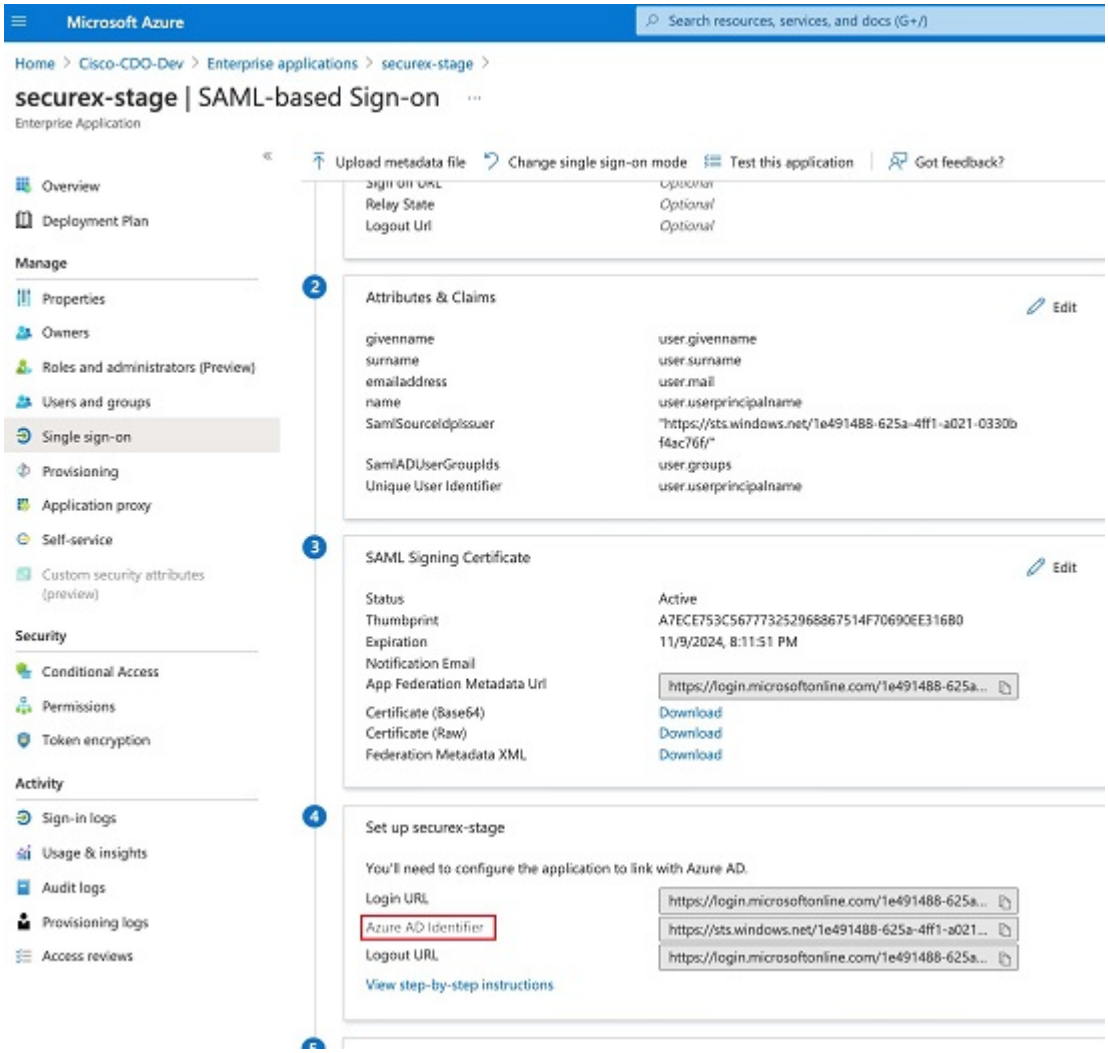
- **SamlADUserGroupIds** - This attribute describes all group associations that a user has on Active Directory. For example, in Azure select **+ Add a group claim** as seen in the screenshot below:

*Figure 2: Custom Claims Defined in Active Directory*




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

*Figure 3: Locate the Azure Active Directory Identifier*




# Add an Active Directory Group for User Management

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

### Procedure

**Step 1** Log in to CDO.

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

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

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

**Step 5** Provide the following information:

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

**Step 6** Select **OK**.

# Edit an Active Directory Group for User Management

### Before you begin

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

### Procedure

**Step 1** Log in to CDO.

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

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

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

**Step 5** Modify the following values:

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

**Step 6** Click **OK**.

# Delete an Active Directory Group for User Management

**Procedure**

**Step 1** Log in to CDO.

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

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

**Step 4** Identify the Active Directory Group you want to delete.

**Step 5** Click the delete icon.

**Step 6** Click **OK** to confirm you want to delete the Active Directory group.

# Create a New CDO User

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

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

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

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

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

### About Logging in to CDO

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

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

**Important** **If your CDO tenant existed before October 14, 2019**, use Migrate to Cisco Security Cloud Sign On Identity Provider, on page 4 for log in instructions instead of this article.

# Before You Log In

### Install DUO Security

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

### Time Synchronization

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

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

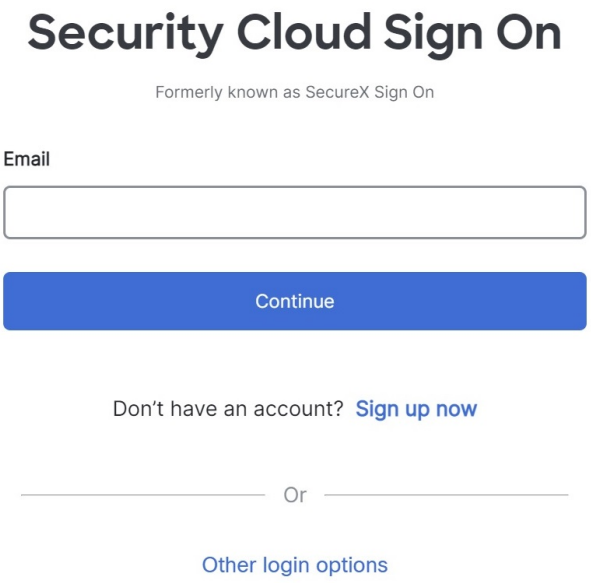
The initial sign-on workflow is a four-step process. You need to complete all four steps.

### Procedure

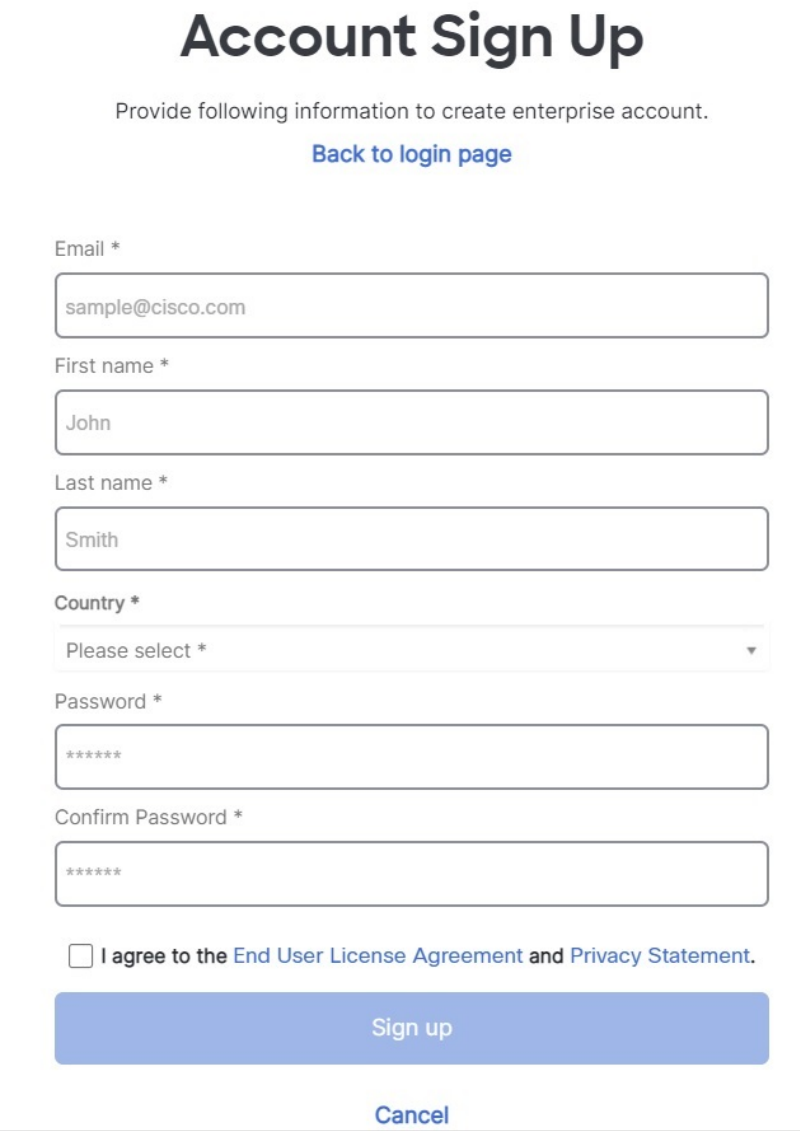
**Step 1** **Sign Up for a New Cisco Security Cloud Sign On Account**.

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

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




**c.** Provide the following information to create enterprise account.




Here are some tips:

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

**d.** Click **Sign up**.

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

**Step 2** **Set up Multi-factor Authentication Using Duo**

We recommend using a mobile device when setting up multi-factor authentication.

**a.** In the **Set up multi-factor authentication** screen, click **Configure factor**.

b. Click **Start setup** and follow the prompts to choose a mobile device and verify the pairing of that mobile device with your account.

   For more information, see Duo Guide to Two Factor Authentication: Enrollment Guide. If you already have the Duo app on your device, you'll receive an activation code for this account. Duo supports multiple accounts on one device.

c. At the end of the wizard click **Continue to Login**.

d. Log in to Cisco Security Cloud Sign On with the two-factor authentication.

**Step 3** **(Optional) Setup Google Authenticator as an additional authenticator**

a. Choose the mobile device you are pairing with Google Authenticator and click **Next**.

b. Follow the prompts in the setup wizard to setup Google Authenticator.

**Step 4** **Configure Account Recovery Options for your Cisco Security Cloud Sign On**

a. Choose a recovery phone number for resetting your account using SMS.

b. Choose a security image.

c. Click **Create My Account**.

# Create a User Record with Your CDO Username

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

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

**Procedure**

**Step 1** Login to CDO.

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

**Step 3** Click + to add a new user to your tenant.

**Step 4** Provide the email address of the user.

**Note** The user's email address must correspond to the email address of the Cisco Secure Log-On account.

**Step 5** From the **Role** drop-down list, select the user's User Roles in CDO.

**Step 6** Click **OK**.

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

### Procedure

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

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

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

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

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

# User Roles in CDO

There are a variety of user roles in CDO: Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a CDO user has access to more than one tenant, they may have the same user ID but different roles on different tenants. A user may have a read-only role on one tenant and a Super Admin role on another. When the interface or the documentation refers to a Read-only user, an Admin user, or a Super Admin user we are describing that user's permission level on a particular tenant.

## Read-only Role

A user assigned the Read-Only role sees this blue banner on every page:

Read Only User. You cannot make configuration changes.

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

- View any page or any setting in CDO.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a read-only user revokes their own token, they cannot recreate it.
- Contact support through our interface and can export a change log.

Read-Only users **cannot** do the following:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create CDO user records.
- Change user role.
- Attach or detach access rules to a policy.

## Edit-Only Role

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

- Edit and save device configurations, including but not limited to objects, policies, rulesets, interfaces, VPN, etc.
- Allow configuration changes that are made through the **Read Configuration** action.
- Utilize the Change Request Management action.

Edit-Only users **cannot** do the following:

- Deploy changes to a device or to multiple devices.
- Discard staged changes or changes that are detected through OOB.
- Upload AnyConnect Packages, or configure these settings.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create CDO user records.
- Change user role.

# Deploy-Only Role

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

- Deploy staged changes to a device, or to multiple devices.
- Revert or restore configuration changes for ASA devices.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Utilize the Change Request Management action.

Deploy-Only users **cannot** do the following:

- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create, update, configure, or delete anything on any page.

- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create CDO user records.
- Change user role.
- Attach or detach access rules to a policy.

# VPN Sessions Manager Role

The VPN Sessions Manager role is designed for administrators monitoring remote access VPN connections, not site to site VPN connections.

Users with the VPN Sessions Manager role can do the following:

- View any page or any setting in CDO.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see RA VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a VPN Sessions Manager user revokes their own token, they cannot recreate it.
- Contact support through our interface and export a change log.
- Terminate existing RA VPN sessions.

VPN Sessions Manager users **cannot** do the following:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create CDO user records.
- Change user role.
- Attach or detach access rules to a policy.

# Admin Role

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

- Create, read, update, and delete any object or policy in CDO and configure any setting.
- Onboard devices.
- View any page or any setting in CDO.
- Search and filter the contents of any page.

- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can contact support through our interface and can export a change log.

Admin users **cannot** do the following:

- Create CDO user records.
- Change user role.

# Super Admin Role

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

- Change a user role.
- Create user records.

**Note** Though Super Admins can create a CDO user record, that user record is not all that is needed for a user to log in to your tenant. The user also needs an account with the identity provider used by your tenant. Unless your enterprise has its own single sign-on identity provider, your identity provider is Cisco Security Cloud Sign On. Users can self-register for their Cisco Security Cloud Sign On account; see Initial Login to Your New CDO Tenant, on page 3 for more information.

- Create, read, update, and delete any object or policy in CDO and configure any setting.
- Onboard devices.
- View any page or any setting in CDO.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can
- Contact support through our interface and can export a change log.

# Change The Record of the User Role

The user record is the currently recorded role of a user. By looking at the users associated with your tenant, you can determine what role each use has by their record. By changing a user role, you change the user record. User's roles are identified by their role in the User Management table. See Manage Users in CDO for more information.

You must be a Super Admin to change the user record. If your tenant has no Super Admins, contact Cisco Defense Orchestrator support.

# 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:

**Procedure**

**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

**Procedure**

**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:

**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:

**Procedure**

**Step 1** Log in to CDO.

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

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

**Step 4** Click **OK**.

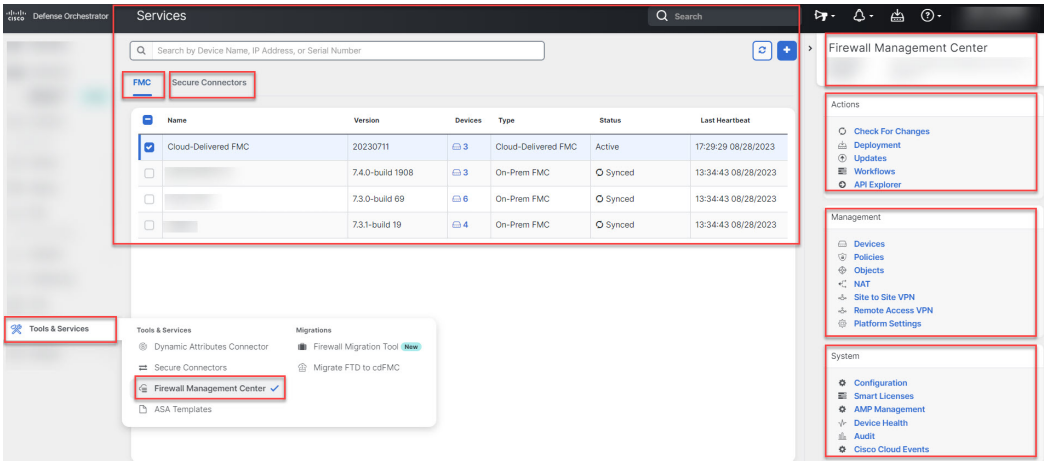
**Step 5** Confirm that you want to remove the account from the tenant by clicking OK.

# CDO Services Page

The **Services** page displays a list of services that CDO provides. Selecting the **FMC** tab lists the cloud-delivered Firewall Management Center that is linked to the CDO account and all the on-prem management centers onboarded to CDO. The devices that are managed by these on-prem management centers are listed in the **Inventory** page. The **Services** page also lists the secure connectors under the **Secure Connectors** tab.

You can click the **FMC** tab and onboard an on-prem management center by clicking the blue plus icon ( ), and perform device actions using the options in the right pane. You can also see device information such as version, number of devices being managed by the management center, device type, and the synchronization status of the device. Clicking on the managed devices icon takes you to the **Inventory** page, where devices managed by the selected on-prem management center are filtered automatically and displayed. The **Services** page also allows you to select more than one on-prem management center at a time for you to perform actions on a group of management centers all at once. You cannot select any on-prem management center while the cloud-delivered Firewall Management Center is selected. To add a new secure connector or perform actions on existing secure connectors, choose the **Secure Connectors** tab and click .

Navigate **Tools & Services** > **Firewall Management Center**.




For your cloud-delivered Firewall Management Center, the Services page displays the following information:

- If you do not have a cloud-delivered Firewall Management Center deployed on your tenant, click **Enable Cloud-Delivered FMC**. See Enable Cloud-Delivered Firewall Management Center on Your CDO Tenant for more information.
- The number of Secure Firewall Threat Defense devices deployed on the cloud-delivered Firewall Management Center.
- Status of the connection between CDO and the cloud-delivered Firewall Management Center page.
- The last heartbeat of the cloud-delivered Firewall Management Center. This represents the last time the status of the cloud-delivered Firewall Management Center itself and the number of devices that it manages were synchronized with the table on this page.
- The hostname of the selected cloud-delivered Firewall Management Center.

Choose **Cloud-Delivered FMC** and using the links in the **Actions**, **Management**, or **Settings** pane, you open the cloud-delivered Firewall Management Center user interface to perform the configuration tasks that are associated with the link you clicked.

**Actions**:

- **Check For Changes**: The Device Count and Status information in the table will be updated with the information available the last time this page and the cloud-delivered Firewall Management Center were synchronized. Synchronization happens every 10 minutes.
- **Deployment**: Takes you to the device configuration deployment page on cloud-delivered Firewall Management Center. See Deploy Configuration Changes.
- **Workflows**: Takes you to the **Workflows** page to monitor every process that CDO runs when communicating with devices. See Workflows page.
- **API Explorer**: Takes you to the page that lists the cloud-delivered Firewall Management Center REST APIs. See Secure Firewall Management Center REST API Guide.

**Management**:

- **Devices**: Takes you to the threat defense device listing page on the cloud-delivered Firewall Management Center portal. See Configure Devices.
- **Policies**: Takes you to the policies page on the cloud-delivered Firewall Management Center portal to edit system-provided access control policies and create custom access control policies. See Manage Access Control Policies.
- **Objects**: Takes you to the policies page on the cloud-delivered Firewall Management Center portal to manage reusable objects. See Object Management.
- **NAT**: Takes you to the policies page on the cloud-delivered Firewall Management Center portal to configure Network Address Translation policies on the threat defense devices. See Manage NAT policies.
- **Site to Site VPN**: Takes you to the site-to-site VPN dashboard page on the cloud-delivered Firewall Management Center portal to configure site-to-site VPN policy between two sites. See Site-to-Site VPNs.
- **Remote Access VPN**: Takes you to the remote access VPN dashboard page on the cloud-delivered Firewall Management Center portal to configure a remote access VPN configuration. See Remote Access VPN.
- **Platform Settings**: Takes you to the platform settings page on the cloud-delivered Firewall Management Center portal configure a range of unrelated features whose values you might want to share among several devices. See Platform Settings.

**System**:

- **Configuration**: Takes you to the system configuration settings page on the cloud-delivered Firewall Management Center portal to configure system configuration settings. See System Configuration.
- **Smart Licenses**: Takes you to the smart licenses page on the cloud-delivered Firewall Management Center portal to assign licenses to devices. See Assign Licenses to Devices.
- **AMP Management**: Takes you to the AMP management page on the cloud-delivered Firewall Management Center portal that provides intelligence that the system uses to detect and block malware on your network. See Cloud Connections for Malware Protection.
- **Device Health**: Takes you to the health monitoring page on the cloud-delivered Firewall Management Center portal that tracks various health indicators to ensure that the hardware and software in the system are working correctly. See About Health Monitoring.
- **Audit**: Takes you to the audit log page on the cloud-delivered Firewall Management Center portal to show the generated audit record for each user interaction with the web interface.
- **Cisco Cloud Events**: Takes you to the configure Cisco Cloud events page on the CDO portal to configure cloud-delivered Firewall Management Center to send events directly to SAL (SaaS). See Send Events to SAL (SaaS).

After opening the cloud-delivered Firewall Management Center page, click the blue question mark button and select **Page-level Help** to learn more about the page you are on and what further action you can take.

### Support to Open CDO and Cloud-delivered Firewall Management Center Applications on Different Tabs

As you configure threat defense devices or objects in the cloud-delivered Firewall Management Center, you can open the appropriate configuration pages in additional browser tabs to work simultaneously in the CDO and the cloud-delivered Firewall Management Center portals without logging off. For example, you can create

an object on the cloud-delivered Firewall Management Center and simultaneously monitor event logs on CDO that are generated from the security policies.

This feature is available for all CDO links that navigate to the cloud-delivered Firewall Management Center portal. To open the cloud-delivered Firewall Management Center portal in a new tab:

On the CDO portal, press and hold the **Ctrl** (Windows) or **Command** (Mac) button, then click the corresponding link.

**Note** A single click opens the cloud-delivered Firewall Management Center page in the same tab.

Here are some examples of opening the cloud-delivered Firewall Management Center portal page in a new tab:

- Choose **Tools & Services** > **Firewall Management Center** and select **Cloud-Delivered FMC**.

  In the right pane, press and hold the **Ctrl** (Windows) or **Command** (Mac) button, and then click the page that you want to access.

- Choose **Objects** > **Other FTD Objects**.

- Click the search icon in the top-right corner of the CDO page and enter the search strings in the search field that appears.

  From the search result, press and hold the **Ctrl** (Windows) or **Command** (Mac) button, and then click the arrow icon.

- Choose **Dashboard** > **Quick Actions**.

  Press and hold the **Ctrl** (Windows) or **Command** (Mac) button, and then click **Manage FTD Policies** or **Manage FTD Objects**.

**Note** When you switch to a new CDO tenant, the corresponding cloud-delivered Firewall Management Center portal already opened in a new tab logs out.

**Related Topics**

- Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator
- Onboard an On-Prem Firewall Management Center
- Request a cloud-delivered Firewall Management Center for your CDO tenant
- Secure Device Connector
- Secure Event Connectors

# CDO Device and Service Management

CDO provides the ability to view, manage, filter, and evaluate your onboarded devices on the **Inventory** page. From the **Inventory** page you can:

- Onboard devices and services for CDO management.
- View the configuration state and connectivity state of managed devices and services.
- View onboarded devices and templates categorized in separate tabs. See CDO Inventory Information, on page 88.
- 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 90.
- Filter for a device or template filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. See Filters.

# Changing a Device's IP Address in CDO

When you onboard an device to Cisco Defense Orchestrator using an IP address, CDO stores that IP address in its database and communicates with the device using that IP address. If the IP address of the device changes, you can update the IP address stored in CDO to match the new address. Changing the device's IP address on CDO does not change device's configuration.

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

**Procedure**

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

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

**Step 3** Click the appropriate device type tab.

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

**Step 4** Select the device whose IP address it is you want to change.

**Step 5** Above the **Device Details** pane, click the edit button next to the device's IP address.

**Step 6** Enter the new IP address in the field and click the blue check button.

No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

**Related Information:**

- Moving Devices Between Tenants, on page 87
- Bulk Reconnect Devices to CDO, on page 86

# Changing a Device's Name in CDO

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

### Procedure

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

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

**Step 3** Select the device whose name it is you want to change.

**Step 4** Above the **Device Details** pane, click the edit button next to the device's name.

**Step 5** Enter the new name in the field and click the blue check button.

No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

# Export a List of Devices and Services

This article explains how to export your list of devices and services to a comma-separated value (.csv) file. Once in that format, you can open the file in a spreadsheet application such as Microsoft Excel to sort and filter the items in your list.

The export button is available in the devices and the templates tab. You are also allowed to export details from devices under the selected device type tab.

Before you export your list of devices and services, look at the filter pane and determine if the Inventory table is displaying the information you want to export. Clear all your filters to see all of your managed devices and services, or filter the information to display a subset of all your devices and services. The export function exports what you can see in the Inventory table.

### Procedure

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

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

**Step 3** Click the appropriate device type tab to export details from devices under that tab or click **All** to export details from all devices.

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

**Step 4** Click **Export list to CSV**:

**Step 5** If prompted, save the .csv file.

**Step 6** Open the .csv file in a spreadsheet application to sort and filter the results.

# Export Device Configuration

You can only export one device configuration at a time. Use the following procedure to export a device's configuration to a JSON file:

**Procedure**

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

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

**Step 3** Click the appropriate device type tab.

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

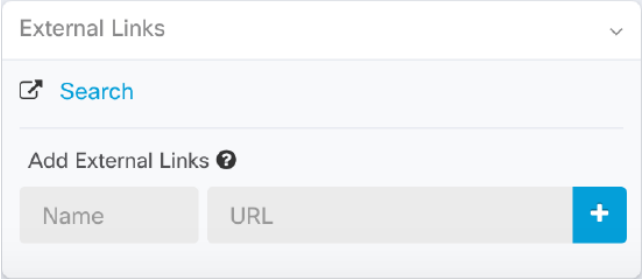
**Step 4** Select the device you want so it is highlighted.

**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 88
- Export a List of Devices and Services, on page 82

## Create an External Link from your Device

### Procedure

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

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

**Step 3** Click the 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.

### Procedure

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

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

**Step 3** Click the 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

### Procedure

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

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

**Step 3** Click the appropriate device type tab.

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

**Step 4** Select multiple devices or models.

**Step 5** In the details pane, on the right, go to the **External Links** section.

**Step 6** Enter a name for the link.

**Step 7** Enter the URL you want to reach using one of these methods:

- Enter

  ```
  https://{location}
  ```

  in the URL field. The {location} variable will be populated with the IP address of your device. This creates an automatic link to the ASDM for your device.

- Enter the URL for the link in the URL field. You need to specify the full URL, for example, for Cisco enter http://www.cisco.com.

**Step 8** Click + to associate the link with the device.

## Edit or Delete External Links

**Procedure**

**Step 1** In the 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

**Procedure**

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

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

**Step 3** Click the 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.

**Procedure**

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

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

**Step 3** Click the appropriate device type tab.

Use the Filters to look for devices whose connectivity status is "unreachable."

**Step 4** From the filtered results, select the devices you want to attempt to reconnect.

**Step 5** Click **Reconnect** . Notice that CDO only provides command buttons for actions that can be applied to all the selected devices.

**Step 6** Look at the **notifications** tab for the progress of the bulk device reconnect action. If you want more information about how the actions in the bulk device reconnect job succeeded or failed, click the blue Review link and you will be directed to the Monitor Jobs in CDO.

**Tip** If a reconnect failure was caused because the device's certificate or credentials have changed, you will have to reconnect to those devices individually to add the new credentials and accept the new certificate.

# Moving Devices Between Tenants

Once you have onboarded devices to a CDO tenant, you cannot migrate the devices from one CDO tenant to another. If you want to move your devices to a new tenant, you need to remove the devices from the old tenant and re-onboard them to the new tenant.

# Device Certificate Expiry Detection

The management certificate is used for accessing FDM-managed and ASA devices from CDO, while the Cisco Secure Client (formerly AnyConnect) is necessary for using virtual private network features on ASA, FDM-managed, and FTD devices from CDO.

CDO actively monitors the expiration status of these certificates and notifies the user when these certificates are nearing their expiration date or have expired. This prevents any disruptions in device operations due to certificate expiry. You should renew the corresponding certificate to address this issue.

The management certificate expiry check applies to ASA and FDM-managed devices, while the Secure Client certificate expiry check applies to ASA, FDM-managed, and FTD devices.

### View Certificate Expiry Notification

In the top right corner, click the **Notifications** ( ) icon to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The **High Priority** section displays the certificate expiration notifications.

These notifications are sent 30, 14, and 7 days before the certificate expiration date and then every day thereafter until the certificate either expires or is renewed with a valid certificate. You can also subscribe to receive these notifications by email on the **Notification Settings** section of the user preferences page. For more information, see User Notification Preferences.

# Write a Device Note

Use this procedure to create a single, plain-text, note file for a device.

**Procedure**

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

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

**Step 3** Click the 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:

**Procedure**

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

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

**Step 3** Click the appropriate device type tab.

**Step 4** Select one or more devices or model in the generated table.

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

**Step 6** Click blue + icon.

# Filters

You can use many different filters on the **Inventory** and **Objects** pages to find the devices and objects you are looking for.

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

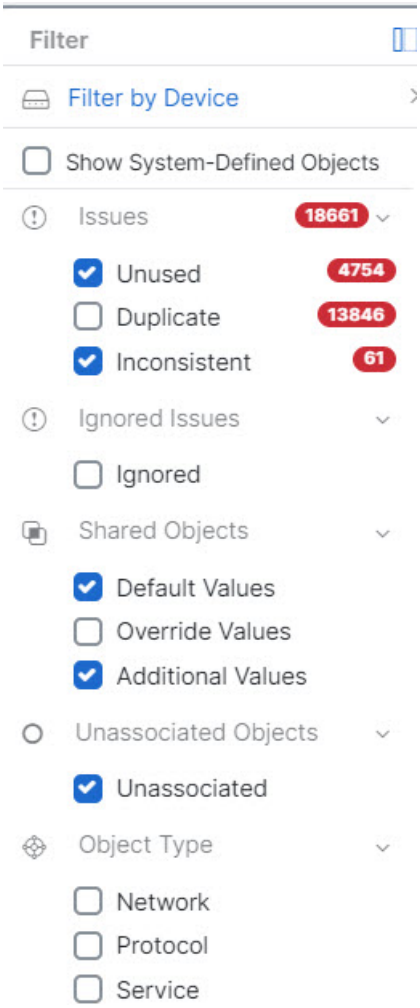
The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters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

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

The object type filter allows you to filter objects by type, such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter allows filtering objects having default values or override values.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values.




# Use CDO Search Functionality

The CDO platform has a highly efficient search function that makes it easy to find anything you need. The search bar on each page is tailored to the content of that page, while the global search allows for a comprehensive search across the entire tenant. This saves time and effort, as you can quickly locate the necessary information.

## Page Level Search

The page-level search enables you to search specific items on the Inventory, Policies, Objects, VPN, Change Log, and Jobs pages.

- In the **Inventory** space, you can simply start typing in the search bar, and devices that fit the search criteria will be displayed. You can type any partial part name of the device, IP address, or the serial number of the physical device to find the device.
- In the **Policies** space, you can search policies by their name, components or objects used in them.

- In the **Objects** space, you can search for an object by typing any partial part of the name of the object, or partial IP Address, port, or protocols.
- In the **VPN** space, you can search by tunnel name, device name, and IP address used in the VPN policies.
- In the **Change log** space, you can search logs based on events, device names, or actions.

**Procedure**

**Step 1** Navigate to the search bar near the top of the interface.

**Step 2** Type the search criteria into the Search Bar and the corresponding results will be displayed.

# Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, CDO recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

CDO calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon:
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy. Before 28 June 2024, when you use an unassociated object in a rule or policy, CDO created a copy of it and used the copy. Because of this behavior, you might have observed that there were two instances of the same object in the **Objects** menu. However, CDO does not do that anymore. You can use an unassociated object in a rule or a policy but there are no duplicate objects that CDO creates.

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

CDO allows you to manage network and service objects across supported devices from one location. With CDO, you can manage objects in these ways:

- Search for and Object Filters based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects in use by a device after it has been on-boarded to CDO.

**Note** Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes on devices, see Out-of-Band Changes on Devices.

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

# Object Types

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

***Table 2: Common Objects***

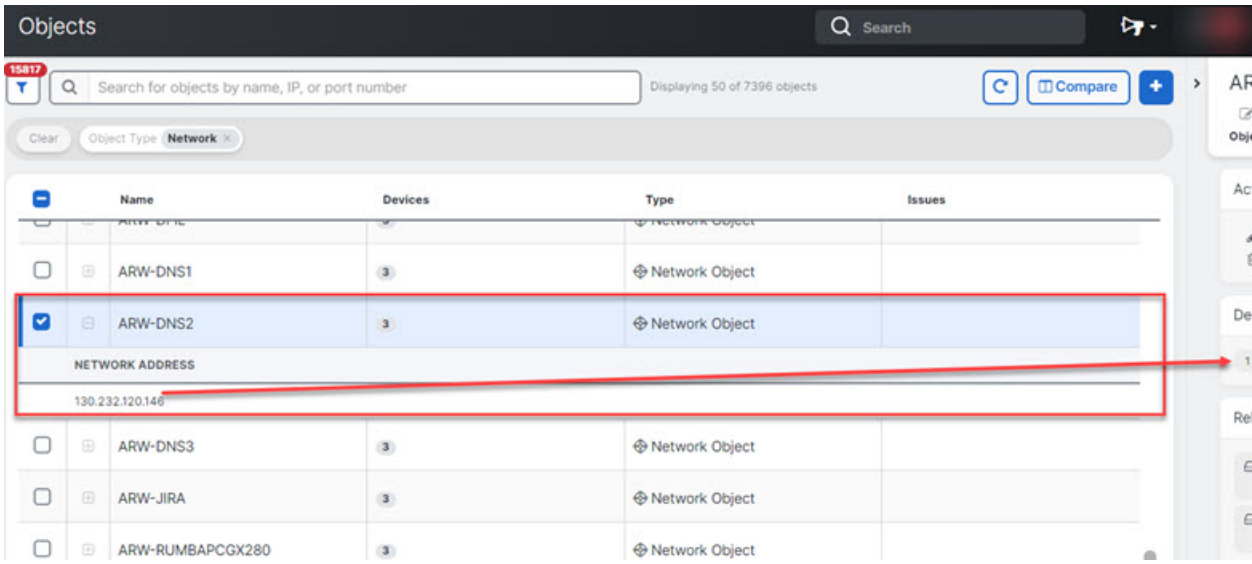
| Object Type | Description |
|---|---|
| Network | Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks. |
| URL | Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies. |

# Shared Objects

Cisco Defense Orchestrator (CDO) calls objects on multiple devices with the same name and same contents, **shared objects**. Shared objects are identified by this icon

on the **Objects** page. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

When looking at a shared object, CDO shows you the contents of the object in the object table. Shared objects have exactly the same contents. CDO shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.



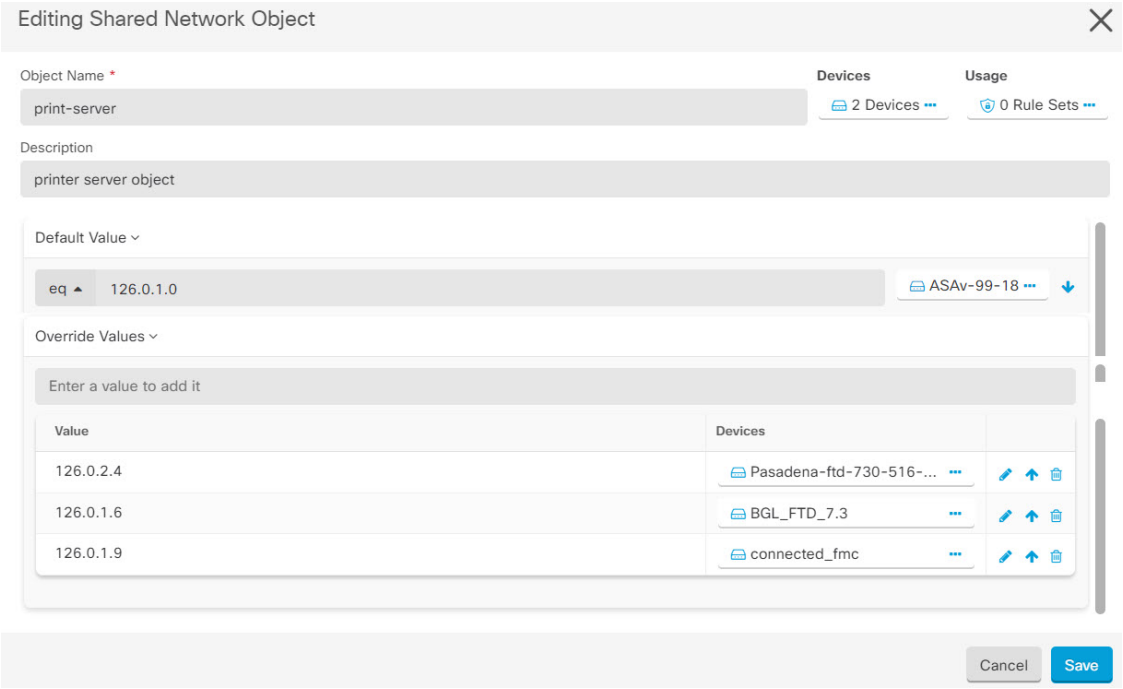

# Object Overrides

An object override allows you to override the value of a shared network object on specific devices. CDO uses the corresponding value for the devices that you specify when configuring the override. Although the objects are on two or more devices with the same name but different values, CDO doesn't identify them as **Inconsistent objects** only because these values are added as overrides.

You can create an object whose definition works for most devices, and then use overrides to specify modifications to the object for the few devices that need different definitions. You can also create an object that needs to be overridden for all devices, but its use allows you to create a single policy for all devices. Object overrides allow you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices.

For example, consider a scenario where you have a printer server in each of your offices, and you have created a printer server object `print-server`. You have a rule in your ACL to deny printer servers from accessing the internet. The printer server object has a default value that you want to change from one office to another. You can do this by using object overrides and maintain rule and "printer-server" object consistent across all locations, although their values may be different.

Out-of-band changes that are done to objects are detected as overrides to the object. When such a change happens, the edited value gets added to the object as an override, which can be viewed by selecting the object. To know more about out-of-band changes, see Out-of-Band Changes on Devices.



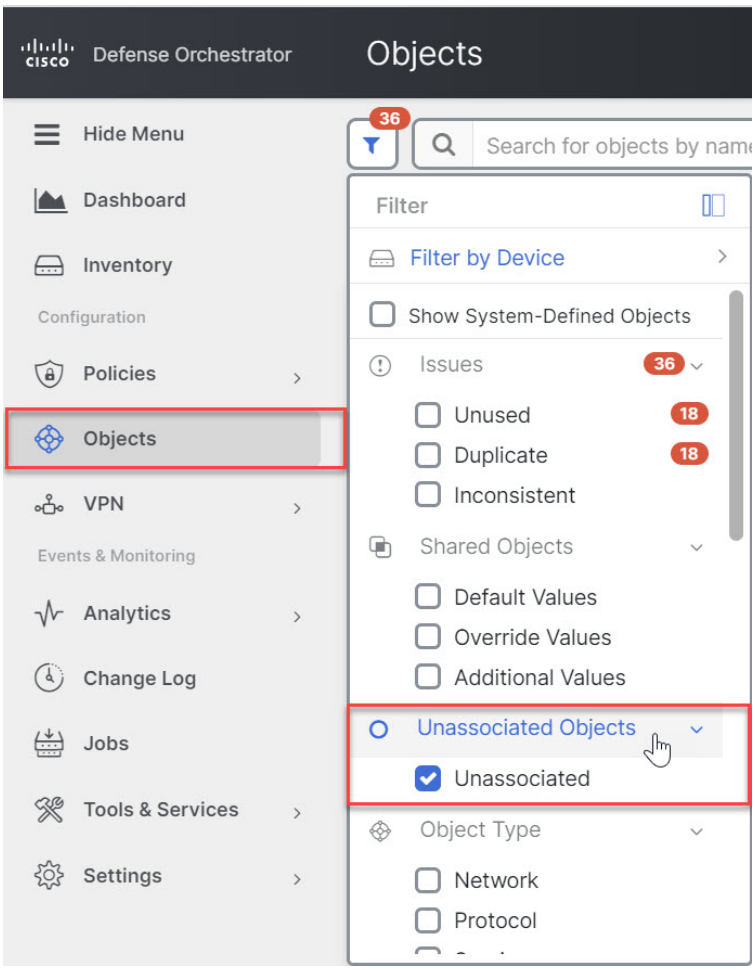

**Note** If there are inconsistent objects, you can combine them into a single shared object with overrides. For more information, see Resolve Inconsistent Object Issues.

# 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.

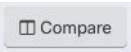



# Compare Objects

**Procedure**

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

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

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

.

**Step 4** Select up to three objects to compare.

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

- Click the up and down arrows in the Object Details title bar to see more or less of the Object Details.
- Expand or collapse the Details and Relationships boxes to see more or less information.

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

to see the configuration of the device. CDO shows you the device's configuration file and highlights the entry for that object.

# Filters

You can use many different filters on the **Inventory** and **Objects** pages to find the devices and objects you are looking for.

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

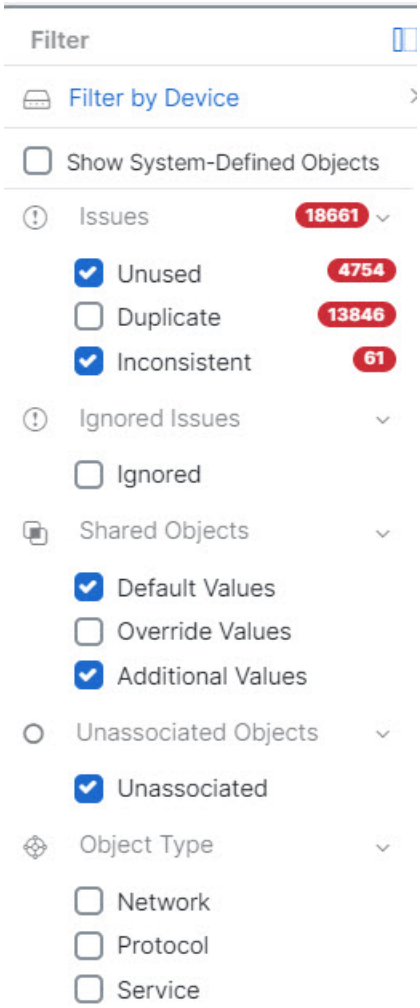
The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters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

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

The object type filter allows you to filter objects by type, such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter allows filtering objects having default values or override values.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values.




## Object Filters

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

- **Filter by Device**: Lets you pick a specific device so that you can see objects found on the selected device.
- **Issues**: Lets you pick unused, duplicate, and inconsistent objects to view.
- **Ignored Issues**: Lets you view all the objects whose inconsistencies you had ignored.
- **Shared Objects**: Lets you view all the objects that CDO has found to be shared on more than one device. You can choose to see shared objects with only default values or override values, or both.
- **Unassociated Objects**: Lets you view all the objects that are not associated with any rule or policy.
- **Object Type**: Lets you select an object type to see only those type of objects that you have selected, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

**Sub filters** – Within each main filter, there are sub-filters you can apply to further narrow down your selection. These sub-filters are based on Object Type – Network, Service, Protocol, etc.

The selected filters in this filter bar would return objects that match the following criteria:

* Objects that are on one of two devices. (Click **Filter by Device** to specify the devices.) AND are

* **Inconsistent** objects AND are

* **Network** objects OR **Service** objects AND

* Have the word "**group**" in their object naming convention

Because **Show System Objects** is checked, the result would include both system objects and user-defined objects.

#### Show System-Defined Objects Filter

Some devices come with pre-defined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

**Show System-Defined Objects** is **off** by default. To display system objects in the object table, check **Show System-Defined Objects** in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

If you hide system objects, they will not be included in your search and filtering results. If you show system objects, they will be included in your object search and filtering results.

## Configure Object Filters

You can filter on as few or as many criteria as you want. The more categories you filter by, the fewer results you should expect.

### Procedure

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

**Step 2** Open the filter panel by clicking the filter icon at the top of the page. Uncheck any filters that have been checked to make sure no objects are inadvertently filtered out. Additionally, look at the search field and delete any text that may have been entered in the search field.

**Step 3** If you want to restrict your results to those found on particular devices:

**a.** Click **Filter By Device**.

**b.** Search all the devices or click a device tab to search for only devices of a certain kind.

**c.** Check the device you want to include in your filter criteria.

**d.** Click **OK**.

**Step 4** Check **Show System Objects** to include system objects in your search results. Uncheck **Show System Objects** to exclude system objects from your search results.

**Step 5** Check the object **Issues** you want to filter by. If you check more than one issue, objects in any of the categories you check are included in your filter results.

**Step 6** Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.

**Step 7** Check the required filter in **Shared Objects** if you are filtering for objects shared between two or more devices.

- **Default Values**: Filters objects having only the default values.

- **Override Values**: Filters objects having overridden values.
- **Additional Values**: Filters objects having additional values.

**Step 8** Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.

**Step 9** Check the **Object Types** you want to filter by.

**Step 10** You can also add an object name, IP address, or port number to the Objects search field to find objects with your search criteria among the filtered results.

### When to Exclude a Device from Filter Criteria

When adding a device to filtering criteria, the results show you the objects on a device but not the relationships of those objects to other devices. For example, assume **ObjectA** is shared between ASA1 and ASA2. If you were to filter objects to find shared objects on ASA1, you would find **ObjectA** but the **Relationships** pane would only show you that the object is on ASA1.

To see all the devices to which an object is related, don't specify a device in your search criteria. Filter by the other criteria and add search criteria if you choose to. Select an object that CDO identifies and then look in the Relationships pane. You will see all the devices and policies the object is related to.

# Unignore Objects

One way to resolve unused, duplicate, or inconsistent objects is to ignore them. You may decide that though an object is unused, a duplicate, or inconsistent, 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.

### Procedure

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

**Step 2** Object Filters.

**Step 3** In the **Object** table, select the object you want to unignore. You can unignore one object at a time.

**Step 4** Click **Unignore** in the details pane.

**Step 5** Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

# Deleting Objects

You can delete a single object or mulitple objects.

## Delete a Single Object

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

Changes you make to network objects and groups on the 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.

**Procedure**

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

**Step 2** Locate the object you want to delete by using object filters and the search field, and select it.

**Step 3** Review the **Relationships** pane. If the object is used in a policy or in an object group, you cannot delete the object until you remove it from that policy or group.

**Step 4** In the Actions pane, click the **Remove** icon .

**Step 5** Confirm that you want to delete the object by clicking **OK**.

**Step 6** Review and deploy the changes you made, or wait and deploy multiple changes at once.

## Delete a Group of Unused Objects

As you onboard devices and start resolving object issues, you find many unused objects. You can delete up to 50 unused objects at a time.

**Procedure**

**Step 1** Use the **Issues** filter to find **unused** objects. You can also use the Device filter to find objects that are not associated with a device by selecting **No Device**. Once you have filtered the object list, the object checkboxes appear.

**Step 2** Check the **Select all** checkbox in the object table header to select all the objects found by the filter that appear in the object table; or, check individual checkboxes for individual objects you want to delete.

**Step 3** In the Actions pane, click the **Remove** icon .

**Step 4** Review and deploy now the changes you made, or wait and deploy multiple changes at once.

# Network Objects

**A network object** can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. **Network groups** are collections of network objects and other individual addresses or subnetworks you add to the group. Network objects and

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

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

### 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, contact 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 contact 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.

# 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 99