Troubleshooting

This chapter covers the following sections:

Troubleshoot FDM-Managed Devices

Use the following article to troubleshoot your FDM-managed devices:

- Troubleshooting Device Registration Failure during Onboarding with a Registration Key

Troubleshoot the Executive Summary Report

You may go to generate a Network Operations Report and not see the results you are expecting, or any data at all. In some cases, the summaries may display **No data available**. Consider the following scenarios:

- CDO polls for events every **hour** from the time the device is onboarded. Some scheduled events can trigger multiple jobs that are polled at varying time intervals, from every 10 minutes, 60 minutes, 6 hours, or 24 hours. If the selected devices have just been onboarded, there may not be enough time to collect and compile data.

- You may have insufficient smart licenses. Only devices that have sufficient licenses generate data. See FDM-Managed Device Licensing Types to determine which smart licenses you required to generate the desired data.

- Logging is not enabled for access control rules. See Logging Settings in an FDM-Managed Access Control Rule for more information.

- The time range you selected may have an insufficient amount of data to display, or an access control rule may not have been triggered within the selected time range. Toggle between the **Time Range** options and determine if a different time period affects the report.

Troubleshoot FDM-Managed Device Onboarding

Connectivity

- Check device connectivity with a ping. Try to ping FP management IP address from ASA directly. If the ICMP blocks communication from outside, you will not be able to ping FP management interface from the Internet. cUrl / wget helps to check if FP management interface is accessible on configured IP/Port.

- Check ASA and/or ASDM software versions for compatibility. See Hardware and Software Supported by CDO for more information.

- Use the ASA logs to identify if CDO traffic is blocked by the ASA. Through SSH, attempts to connect to FP HTTP management interface are logged in **/var/log/httpd/httpsd_access_log**.

Module Misconfiguration

- Unsupported configuration. CDO may not be able to support the device's configuration if the module does not meet specific requirements.

HTTP Authentication

- CDO issues an token-based SSO to authenticate an ASA device during the onboarding process. A token issue may be caused by attempt to onboard FP module from non-admin context in case of ASA in multi-context mode. Invalid tokens are identified as **ASDM SSO logins** in **/var/log/mojo/mojo.log a**

Failed Because of Insufficient License

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.

- If the device status doesn't change, refresh the CDO portal by signing out from CDO and signing back to resolve any network communication glitch between license server and device.

- If the portal refresh doesn't change the device status, perform the following:

Procedure

Step 1 Generate a new new registration key from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.

Step 2 In the CDO navigation bar, click the **Inventory** page.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab and select the device with the **Insufficient License** state.

Step 5 In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.

Step 6 In the **Activate** field, paste the new registration key and click **Register Device**.

Once the new registration key is applied successfully to the device, its connectivity state turns to **Online**.

Related Information:

- Onboard an FDM-Managed Device

- Onboard an FDM-Managed Device Using Username, Password, and IP Address

- Applying or Updating a Smart License

Troubleshoot Device Unregistered

The FDM-managed device may have been unregistered from the cloud via Firewall device manager.

Perform the following to register the device again on the cloud:

Procedure

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the **FTD** tab and select the device in the "Device Unregistered" state, and see the error message on the right.

Step 3 If the unregistered device was onboarded using the registration key, Cisco Defense Orchestrator prompts you to generate a new registration key as the previously applied key has expired.

a) Click the Refresh button to generate a new registration key and then click the Copy icon .

b) Log into the Firewall device manager of the device you want to reregister with CDO.

c) Under **System Settings**, click **Cloud Services**.

d) In the Cisco Defense Orchestrator area, expand **Get Started**.

e) In the **Registration Key** field, paste the registration key that you generated in CDO.

f) Click **Register** and then **Accept** the Cisco Disclosure. Firewall device manager sends the registration request to CDO.

g) Refresh the **Inventory** page in CDO until you see the device's connectivity state changes to "Read Error".

h) Click **Read Configuration** for CDO to read the configuration from the device.

Step 4 If the unregistered device was onboarded using the serial number, CDO prompts you to auto-enroll the device from Firewall device manager.

a) Log into the Firewall device manager of the device you want to reregister with CDO.

b) Under **System Settings**, click **Cloud Services**.

c) Select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click **Register**.

d) Refresh the **Inventory** page in CDO until you see the device's connectivity state changes to "Read Error".

e) Click **Read Configuration** for CDO to read the configuration from the device.

Troubleshooting Device Registration Failure during Onboarding with a Registration Key

Failed to Resolve Cloud Service FQDN

If the device registration fails due to failure in resolving cloud service FQDN, check network connectivity or the DNS configuration and attempt to onboard the device again.

Failed Because of an Invalid Registration Key

If the device registration fails due to an invalid registration key, which may occur when you paste incorrect registration key in Firewall device manager.

Copy the same registration key from Cisco Defense Orchestrator again and attempt to register the device. If the device is already smart licensed, ensure that you remove the smart license before pasting the registration key in firewall device manager.

Failed Because of Insufficient License

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.

- If the device status doesn't change, refresh the CDO portal by signing out from CDO and signing back to resolve any network communication problems between license server and device.

- If the portal refresh doesn't change the device status, perform the following:

  1. Generate a new new registration key from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.

  2. In the CDO navigation bar, click the **Inventory** page.

  3. Select the device with the **Insufficient License** state.

  4. In the **Device Details** pane, click **Manage Licenses** appearing in Insufficient Licenses. The Manage Lincenses window opens.

  5. In the **Activate** field, paste the new registration key and click **Register Device**.

- Once the new registration key is applied successfully to the device, its connectivity state turns to **Online**.

Troubleshoot Intrusion Prevention System

What are my IPS policy options?

Every onboarded device is automatically associated a Cisco Defense Orchestrator-provided IPS policy called "Default Overrides". CDO generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. If you want to use the default IPs policy but modify the signature overrides options, see Firepower Intrusion Policy Signature Overrides for more information. Note that configuring different signature overrides per device may cause the default overrides policy to become inconsistent.

How do I have a different IPS policy for every device?

CDO generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. You do not have to rename the CDO-provided IPS policy after each device is onboarded. Expanding the policy displays the devices that are associated with it, and you can also filter the threat events page and the signature overrides page per device or policy. To customize the default overrides policy, configure signature overrides per device. This will cause the default overrides intrusions policy to become inconsistent, but this does not inhibit any functionality.

I onboarded a device that has an override configured from an FDM-managed device.

Overrides that are configured outside of CDO do not pose an issue to device configuration or functionality.

If you onboard a device that has an override already configured and this new device shares an IPs policy with a device that does **not** have an override, the IPS policy will be displayed as **inconsistent**. See Step 3 in Firepower Intrusion Policy Signature Overrides to address inconsistencies.

Troubleshooting SSL Decryption Issues

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

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

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

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

- Support app users, in which case you cannot decrypt any traffic to the site. Create a Do Not Decrypt rule for the site's application (on the Application tab for the SSL Decryption rule) and ensure that the rule comes before any Decrypt Re-sign rule that would apply to the connections.

- Force users to use browsers only. If you must decrypt traffic to the site, you will need to inform users that they cannot use the site's app when connecting through your network, that they must use their browsers only.

More Details

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

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

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the server. The Alert is usually an "Unknown CA (48)" alert indicating SSL Pinning.

A TCP Reset is sent following the Alert message. You should see the following symptoms in the event details:

- SSL Flow Flags include ALERT_SEEN.

- SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.

- SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.

- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is done and then send a TCP Reset. You should see the following symptoms in the event:

  - SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.

  - SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.

Download Button for CA Certificate is Disabled

The download button is disabled for certificates (self signed and uploaded) that are staged on CDO but have not been deployed back to the device yet. A certificate can be downloaded only after deploying it to the device.

Troubleshoot FDM-Managed Device Onboarding Using Serial Number

- Provisioning Error
  - Device Password Has Not Been Changed
  - Device Password Has Already Been Changed

- Claim Error
  - Invalid Serial Number
  - Device Serial Number Already Claimed
  - Device is Offline
  - Failed to Claim the Device

Claim Error

Invalid Serial Number

> ⊗ **Claim Error**
> Failed to claim the device. Invalid serial number –
> JAD213082X9.

An incorrect serial number has been entered while claiming the device in Cisco Defense Orchestrator.

Resolution

1. Delete the FDM-managed device instance in CDO.

2. Create a new FDM-managed device instance by entering the correct serial number and claim the device.

Device Serial Number Already Claimed

The following error occurs when you are onboarding the FDM-managed device using its serial number.

⊗ Claim Error
Device with serial number JAD213082X9 is already claimed.

Cause

This error can occur for one of the following reasons:

- The device may have been purchased from an external vendor, and the device is in the vendor's tenancy.

- The device may have been previously managed by another CDO instance in a different region and is registered to its cloud tenancy.

Resolution

You need to unregister the device's serial number from other cloud tenancy and then reclaim it in your tenant.

Prerequisite

The device must be connected to the Internet that can reach the cloud tenancy.

Device Purchased from an External Vendor

The device purchased from an external vendor may have been registered to the vendor's cloud tenancy.

1. Delete the device instance from CDO.

2. Install the FXOS image on the device. For more information, see the "Reimage Procedures" chapter of the Cisco FXOS Troubleshooting Guide for the Firepower 1000/21000 with FTD guide.

3. Connect to the FXOS CLI from the console port.

4. Log in to FXOS using your current admin password.

5. In the FXOS CLI, connect to local-mgmt: firepower # **connect local-mgmt**.

6. Execute the command to deregister the device from the cloud tenancy. firepower(local-mgmt) # **cloud deregister**.

7. On successful deregistration, the CLI interface returns a success message.

   Example: **firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9**

   If the device was already unregistered from the cloud tenancy, the CLI interface indicates that the device serial number was not registered with cloud tenancy. **RESULT=success MESSAGE=DEVICE_NOT_FOUND: Device with serial number JAD213082x9 is not registered with** Security Services Exchange **, X-Flow-Id: 63e48b4c-8426-48fb-9bd0-25fcd7777b99**

8. Claim the device again in CDO by providing its serial number. See Onboard an FDM-Managed Device using the Device Serial Number for more information.

9. Install the FDM-managed device application (version 6.7 or later) on the device. The low-touch provisioning is initiated on the device and it registers itself in the Cisco Cloud. CDO onboards the device.

Onboard an FDM-Managed Device Already Managed by Another Cloud Tenancy in a Different Region

The device may have been previously managed by another CDO instance in a different region and is registered to its cloud tenancy.

Case 1: You have access to the tenant that owns the device.

1. Delete the device instance from the CDO in region 1.

2. In Firewall device manager, go to **System Settings** > **Cloud Services** page. A warning message appears indicating that the device has been removed from CDO.

3. Click the link and select **Unregister Cloud Services** from the drop-down list.

4. Read the warning and click **Unregister**.

5. Claim the device from CDO in region 2.

6. In Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click **Register**. The device maps to the new tenant that belongs to the new region and CDO onboards the device.

Case 2: You don't have access to the tenant that owns the device.

1. Connect to the FXOS CLI from the console port.

2. Log in to FXOS using your current admin password.

3. In the FXOS CLI, connect to local-mgmt: firepower # **connect local-mgmt**.

4. Execute the command to deregister the device from the cloud tenancy. firepower(local-mgmt) # **cloud deregister**.

5. On successful deregistration, the CLI interface returns a success message.

   Example: **firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9**

   The device is unregistered from the cloud.

6. Claim the device from CDO in region 2.

7. In Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click **Register**. The device maps to the new tenant that belongs to the new region and CDO onboards the device.

Device is Offline

Claim Error
Failed to claim the device. Device with serial number JAD213082X9 is offline. Please try again later.

Cause

The device is unable to reach the Cisco Cloud due to one of the following reasons:

• The device is cabled incorrectly.

• Your network may require a static IP address for the device.

• Your network uses custom DNS, or there is external DNS blocking on the customer network.

• PPPoE authentication is needed. (Common in Europe region.)

• The FDM-managed device is behind a proxy.

Resolution

1. Sign in to the device and go through the bootstrap CLI process or the CDO Easy setup process to configure the device first so it can reach the Internet.

2. Check the cabling and network connectivity.

3. Ensure that your firewall is not blocking any traffic.

4. Ensure that the Security Services Exchange domains are reachable. See Configuration Prerequisites for Hardware Installation for more information.

Failed to Claim the Device

Cause

This error may occur due to one of the following reasons:

• Security Services Exchange may have temporary issues.

• The server may be down.

Resolution

1. Delete the FDM-managed device instance in CDO.

2. Create a new FDM-managed device instance and claim the device again after some time.

Note If you are not able to claim the device, go to the workflows to see the error message and send the details to the CDO support team.

Provisioning Error

Device Password Has Not Been Changed

When claiming the device from Cisco Defense Orchestrator, the device's initial provisioning may fail and display an "Unprovisioned" message in the **Inventory** page.

Cause

You may have selected the "Default Password Changed" option in the CDO FDM-managed device serial number onboarding wizard for a new FDM-managed device whose default password was not changed.

Resolution

You need to click **Enter Password** in the **Inventory** page to change the device's password. CDO continues with the new password and onboards the device.

Device Password Has Already Been Changed

When claiming the device from CDO, the device's initial provisioning may fail and display an "Unprovisioned" message in the **Inventory** page.

Cause

You may have selected the "Default Password Not Changed" option in the CDO FDM-managed device serial number onboarding wizard for an FDM-managed device whose default password has already been changed.

Resolution

You need to click **Confirm and Proceed** in the **Inventory** page to ignore the new password provided in the serial onboarding wizard. CDO continues with the old password and onboards the device.

For Other Errors

For all other provisioning errors, you can click **Retry** to reinitiate the provisioning. If it fails even after multiple retries, perform the following steps:

1. Delete the FDM-managed device instance from CDO and create a new instance. See Onboard an FDM-Managed Device using the Device Serial Number for onboarding steps.

2. In Firewall device manager, go to **System Settings** > **Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click**Register**.

Troubleshoot FDM-Managed HA Creation

Event Description Error

If you attempt to onboard or create an FDM-managed HA pair in Cisco Defense Orchestrator, the HA pair may fail to form and you may see an error with the following message:

Event description: `CD App Sync error is Cisco Threat Response is enabled on Active but not on Standby`

If you see this error, then one or both of the devices within the HA pair is not configured to allow the devices to send events to the a Cisco cloud server such as CDO, Firepower Threat Response, Or the Cisco Success Network.

You **must** enable the **Send Events to the Cisco Cloud** feature from the Firewall device manager UI. See the **Configuring Cloud Services** chapter of the Firepower Device Manager Configuration Guide of the version you are running for more information.

One of my devices is in a bad state after creating HA

If one of the devices falls into an unhealthy or **failed** state during HA creation, break the HA pair and resolve the device's state, then recreate HA. The failover history might help diagnose the issue.

Troubleshoot a Secure Device Connector

Use these topics to troubleshoot an on-premises Secure Device Connector (SDC).

If none of these scenarios match yours, open a case with Cisco Technical Assistance Center.

SDC is Unreachable

An SDC is in the state "Unreachable" if it has failed to respond to two heartbeat requests from CDO in a row. If your SDC is unreachable, your tenant will not be able to communicate with any of the devices you have onboarded.

CDO indicates that an SDC is unreachable in these ways:

- You see the message, "Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs." on the CDO home page.

- The SDC's status in the Services page is "Unreachable."

Frist, attempt to reconnect the SDC to your tenant to resolve this issue:

1. Check that the SDC virtual machine is running and can reach a CDO IP address in your region. See Connect Cisco Defense Orchestrator to your Managed Devices.

2. Attempt to reconnect CDO and the SDC by requesting a heartbeat manually. If the SDC responds to a heartbeat request, it will return to "Active" status. To request a heartbeat manually:

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

    b. Click the SDC that is unreachable.

    c. In the Actions pane, click **Request Heartbeat**.

    d. Click **Reconnect**.

3. If the SDC does not return to the Active status after manually attempting to reconnect it to your tenant, follow the instructions in SDC Status Does not Become Active on CDO after Deployment, on page 11.
.

SDC Status Does not Become Active on CDO after Deployment

If CDO does not indicate that your SDC is active in about 10 minutes after deployment, connect to the SDC VM using SSH using the `cdo` user and password you created when you deployed the SDC.

Procedure

Step 1   Review `/opt/cdo/configure.log`. It shows you the configuration settings you entered for the SDC and if they were applied successfully. If there were any failures in the setup process or if the values weren't entered correctly, run the sdc-onboard setup again:

a) At the `[cdo@localhost cdo]$` prompt enter `sudo sdc-onboard setup`.

b) Enter the password for the `cdo`user.

   c) Follow the prompts. The setup script guides you through all the configuration steps you took in the setup wizard and gives you an opportunity to make changes to the values you entered.

Step 2   If after reviewing the log and running `sudo sdc-onboard setup`, CDO still does not indicate that the SDC is **Active**, contact CDO support.

Changed IP Address of the SDC is not Reflected in CDO

If you changed the IP address of the SDC, it will not be reflected in CDO until after 3:00 AM GMT.

Troubleshoot Device Connectivity with the SDC

Use this tool to test connectivity from CDO, through the Secure Device Connector (SDC) to your device. You may want to test this connectivity if your device fails to onboard or if you want to determine, before on-boarding, if CDO can reach your device.

Procedure

Step 1   From the CDO menu, choose **Tools & Services** > **Secure Connectors**.

Step 2   Select the SDC.

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

Step 4   Enter a valid IP address or FQDN and port number of the device you are attempting to troubleshoot, or attempting to connect to, and click **Go**. CDO performs the following verifications:

   a) **DNS Resolution** - If you provide a FQDN instead of an IP address, this verifies the SDC can resolve the domain name and acquires the IP address.

   b) **Connection Test** - Verifies the device is reachable.

   c) **TLS Support** - Detects the TLS versions and ciphers that both the device and the SDC support.

     • **Unsupported Cipher** - If there are no TLS version that are supported by both the device and the SDC, CDO also tests for TLS versions and ciphers that are supported by the device, but not the SDC.

   d) SSL Certificate - The troubleshoot provides certificate information.

Step 5   If you continue to have issues onboarding or connecting to the device, contact Defense Orchestrator support.

Intermittent or No Connectivity with SDC

The solution discussed in this section applies only to an on-premise Secure Device Connector (SDC).

Symptom: Intermittent or no connectivity with SDC.

Diagnosis: This problem may occur if the disk space is almost full (above 80%).

Perform the following steps to check the disk space usage.

1. Open the console for your Secure Device Connector (SDC) VM.

2. Log in with the username **cdo**.

3. Enter the password created during the initial login.

4. First, check the amount of free disk space by typing **`df -h`** to confirm that there is no free disk space available.

   You can confirm that the disk space was consumed by the Docker. The normal disk usage is expected to be under 2 Gigabytes.

5. To see the disk usage of the **Docker** folder,

   execute **`sudo du -h /var/lib/docker | sort -h`**.

   You can see the disk space usage of the **Docker** folder.

Procedure

If the disk space usage of the Docker folder is almost full, define the following in the docker config file:

   • Max-size: To force a log rotation once the current file reaches the maximum size.

   • Max-file: To delete excess rotated log files when the maximum limit it reached.

Perform the following:

1. Execute **`sudo vi /etc/docker/daemon.json`**.

2. Insert the following lines to the file.

   `{`

   `"log-driver": "json-file",`

   `"log-opts": {"max-size": "100m", "max-file": "5" }`

   `}`

3. Press **ESC** and then type **`:wq!`** to write the changes and close the file.

   Note You can execute **`sudo cat /etc/docker/daemon.json`** to verify the changes made to the file.

4. Execute **`sudo systemctl restart docker`** to restart the docker file.

   It will take a few minutes for the changes to take effect. You can execute **`sudo du -h /var/lib/docker | sort -h`** to see the updated disk usage of the docker folder.

5. Execute **`df -h`** to verify that the free disk size has increased.

6. Before your SDC status can change from Unreachable to Active, you must go to the Secure Connectors tab in the **Services** page from CDO and click **Request Reconnect** from the Actions menu.

Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc

The Cisco Product Security Incident Response Team (PSIRT) published the security advisory **cisco-sa-20190215-runc** which describes a high-severity vulnerability in Docker. Read the entire PSIRT team advisory for a full explanation of the vulnerability.

This vulnerability impacts all CDO customers:

- Customers using CDO's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the CDO Operations Team.

- Customers using an SDC deployed on-premise need to upgrade their SDC host to use the latest Docker version. They can do so by using the following instructions:

  - Updating a CDO-Standard SDC Host, on page 14
  - Updating a Custom SDC Host, on page 15
  - Bug Tracking, on page 15

Updating a CDO-Standard SDC Host

Use these instructions if you deployed an SDC using the CDO image.

Procedure

Step 1 Connect to your SDC host using SSH or the hypervisor console.

Step 2 Check the version of your Docker service by running this command:

```
docker version
```

Step 3 If you are running one of the latest virtual machines (VMs) you should see output like this:

```
 > docker version
Client:
    Version: 18.06.1-ce
    API version: 1.38
    Go version: go1.10.3
    Git commit: e68fc7a
    Built: Tue Aug 21 17:23:03 2018
    OS/Arch: linux/amd64
    Experimental: false
```

It's possible you may see an older version here.

Step 4 Run the following commands to update Docker and restart the service:

```
> sudo yum update docker-ce
> sudo service docker restart
```

Note There will be a brief connectivity outage between CDO and your devices while the docker service restarts.

Step 5 Run the docker version command again. You should see this output:

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

Step 6 You are done. You have now upgraded to the latest, and patched, version of Docker.

Updating a Custom SDC Host

If you have created your own SDC host you will need to follow the instructions to update based on how you installed Docker. If you used CentOS, yum and Docker-ce (the community edition) the preceding procedure will work.

If you have installed Docker-ee (the enterprise edtion) or used an alternate method to install Docker, the fixed versions of Docker may be different. You can check the Docker page to determine the correct versions to install: Docker Security Update and Container Security Best Practices.

Bug Tracking

Cisco is continuing to evaluate this vulnerability and will update the advisory as additional information becomes available. After the advisory is marked Final, you can refer to the associated Cisco bug for further details:

CSCvo33929-CVE-2019-5736: runc container breakout

Invalid System Time

Cisco Defense Orchestrator (CDO) is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, CDO must migrate your existing SDC to the new communication method by February 1, 2024.

Note If your SDC is not migrated by February 1, 2024, CDO will no longer be able to communicate with your devices through the SDC.

CDO's operations team attempted to migrate your SDC but was unsuccessful because your SDC system time was 15 minutes ahead or behind the AWS system time.

Please follow the steps below to correct the system time issue. Once this problem is resolved, we will be able to proceed with the migration.

Procedure

Step 1 Login to your SDC VM throught the VM terminal or by making an SSH connection.

Step 2 At the prompt, enter `sudo sdc-onboard setup` and authenticate.

Step 3 You are now going to respond to the SDC setup questions as if you are were setting up the SDC for the first time. Re-enter all the same passwords and network information as you had before, except take special note of the NTP server address:

    a) Reset the root and cdo user passwords with the same passowrds you used to setup the SDC.

    b) When prompted, enter **y** to re-configure the network.

    c) Enter the value for IP address/CIDR as you had before.

    d) Enter the value for the network gateway as you had before.

    e) Enter the value for the DNS Server as you had before.

    f) When prompted for the NTP server, be sure to provide a valid NTP server address, such as `time.aws.com`.

    g) Review the values you provided and enter **y** if they are correct.

Step 4 Validate that your time server is reachable and synchronized with your SDC by entering `date` at the prompt. The UTC date and time are displayed and you can compare it to your SDC time.

What to do next

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the CDO operations team can complete your SDC migration to the new communication method.

SDC version is lower than 202311****

Cisco Defense Orchestrator (CDO) is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, CDO must migrate your existing SDC to the new communication method by February 1, 2024.

Note If your SDC is not migrated by February 1, 2024, CDO will no longer be able to communicate with your devices through the SDC.

CDO's operations team attempted to migrate your SDC but was unsuccessful because your tenant is running a version lower than 202311****.

The current version of your SDC is listed on the Secure Connectors page by navigating from the CDO menu bar, **Tools & Services** > **Secure Connectors**. After selecting your SDC, its version number is found in the **Details** pane on the right of the screen.

Please follow the steps below to upgrade the SDC version. Once this problem is resolved, CDO operations will be able to run the migration process again.

Procedure

Step 1 Log in to the SDC VM and authenticate.

Step 2 At the prompt, enter `sudo su - sdc` and authenticate.

Step 3 At the prompt, enter `crontab -r`.

If you receive the message `no crontab for sdc` you can ignore it and move to the next step.

Step 4   At the prompt, enter `./toolkit/toolkit.sh upgrade`. CDO will determine if you need an upgrade and upgrade the toolkit. Ensure that no errors were reported in the console.

Step 5   Verify the new version of the SDC:

a) Log in to CDO.

b) Navigate to the Secure Connectors page by navigating from the CDO menu bar, **Tools & Services** > **Secure Connectors**.

c) Select your SDC and click **Request Heartbeat** in the **Actions** pane.

d) Validate that the SDC version is 202311**** or later.

What to do next

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the CDO operations team can run the migration process again.

Certificate or Connection errors with AWS servers

Cisco Defense Orchestrator (CDO) is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, CDO must migrate your existing SDC to the new communication method by February 1, 2024.

✎

Note   If your SDC is not migrated by February 1, 2024, CDO will no longer be able to communicate with your devices through the SDC.

CDO's operations team attempted to migrate your SDC but was unsuccessful because they experienced a connection issue.

Please follow the steps below to correct the connection issue. Once this problem is resolved, we will be able to proceed with the migration.

Procedure

Step 1   Create firewall rules that allow outbound proxy connections, on port 443, to the domains in your region:

• Production tenants in the US region:

• cognito-identity.us-west-2.amazonaws.com

• cognito-idp.us-west-2.amazonaws.com

• sns.us-west-2.amazonaws.com

• sqs.us-west-2.amazonaws.com

• Production tenants in the EU region:

• cognito-identity.eu-central-1.amazonaws.com

• cognito-idp.eu-central-1.amazonaws.com

> • sns.eu-central-1.amazonaws.com
>
> • sqs.eu-central-1.amazonaws.com

- Production tenants in the APJ region:

  > • cognito-identity.ap-northeast-1.amazonaws.com
  >
  > • cognito-idp.ap-northeast-1.amazonaws.com
  >
  > • sqs.ap-northeast-1.amazonaws.com
  >
  > • sns.ap-northeast-1.amazonaws.com

Step 2   You can determine the full list of IP addresses you need to add to your firewall's "allow list" by using one of the commands below.

Note   The commands below are for users that have **jq** installed. The IP addresses will be displayed in a single list.

- Production tenants in the US region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- Production tenants in the EU region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- Production tenants in the APJ region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

Note   If you don't have **jq** installed, you can use this shortened version of the command:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

What to do next

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the CDO operations team can complete your SDC migration to the new communication method.

Secure Event Connector Troubleshooting

If none of these scenarios match yours, open a case with Cisco Technical Assistance Center.

Troubleshooting SEC Onboarding Failures

These troubleshooting topics describes many different symptoms related to Secure Event Connector (SEC) onboarding failure.

SEC on-boarding failed

Symptom: SEC on-boarding failed.

Repair: Remove the SEC and onboard it again.

If you receive this error:

1. Remove the Secure Event Connector and its files from the virtual machine container.

2. Update your Secure Device Connector. Ordinarily, the SDC is updated automatically and you should not have to use this procedure but this procedure is useful in cases of troubleshooting.

3. Install a Secure Event Connector on an SDC Virtual Machine.

Tip Always use the copy link to copy the bootstrap data when on-boarding an SEC.

Note If this procedure does not correct the problem, Event Logging Troubleshooting Log Files and contact your Managed Service Provider or the Cisco Technical Assistance Center.

SEC Bootstrap data not provided

Message: ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

Diagnosis: Boostrap data was not entered into the setup script when prompted.

Repair: Provide the SEC bootstrap data generated in CDO UI when prompted for the bootstrap data input when onboarding.

Bootstrap config file does not exist

Message: ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/cdo/es_bootstrapdata") does not exist, exiting.

Diagnosis: SEC Bootstrap data file("/usr/local/cdo/es_bootstrapdata") is not present.

Repair: Place the SEC bootstrap data generated in CDO UI onto the file **/usr/local/cdo/es_bootstrapdata** and try onboarding again.

1. Repeat onboarding procedure.

2. Copy the bootstrap date.

3. Log into the SEC VM as the 'sdc' user.

4. Place the SEC bootstrap data generated in CDO UI onto the file **/usr/local/cdo/es_bootstrapdata** and try onboarding again.

Decoding bootstrap data failed

Message: ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC boostrap data, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

Diagnosis: Decoding bootstrap data failed

Repair: Regenerate SEC bootstrap data and try onboarding again.

Bootstrap data does not have required information to onboard SEC

Messages:

- ERROR cannot bootstrap Secure Event Connector container for tenant, the Security Services Exchange FQDN not set, exiting.

- ERROR cannot bootstrap Secure Event Connector container for tenant, the Security Services Exchange OTP not set, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: Security
Services
                                    Exchange FQDN not set, exiting.
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: Security
Services
                                    Exchange FQDN not set, exiting.
```

Diagnosis: Bootstrap data does not have required information to onboard SEC

Repair: Regenerate bootstrapdata and try onboarding again.

Toolkit cron currently running

Message: ERROR SEC toolkit already running, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

Diagnosis: Toolkit cron currently running.

Repair: Retry onboarding command again.

Adequate CPU and memory not available

Message: ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

Diagnosis: Adequate CPU and memory not available.

Repair: Ensure minimum of 4 CPUs and 8 GB RAM are provisioned exclusively for SEC on your VM and try onboarding again.

SEC already running

Message: ERROR Secure Event Connector already running, execute 'cleanup' before onboarding a new Secure Event Connector, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

Diagnosis: SEC already running.

Repair: Run SEC Cleanup Command before onboarding a new SEC.

SEC domain unreachable

Messages:

- Failed connect to api-sse.cisco.com:443; Connection refused

- ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

Diagnosis: SEC domain unreachable

Repair: Ensure the on-premise SDC has Internet connectivity and try onboarding again.

Onboarding SEC command succeeded without errors, but SEC docker container is not up

Symptom: Onboarding SEC command succeeded without errors, but SEC docker container is not up

Diagnosis: Onboarding SEC command succeeded without errors, but SEC docker container is not up

Repair:

1. Log in to the SEC as the 'sdc' user.

2. Check for any errors in SEC docker container startup logs(/usr/local/cdo/data/<tenantDir>/event_streamer/logs/startup.log).

3. If so, run SEC Cleanup Command and try onboarding again.

Contact CDO Support

If none of these scenarios match yours, open a case with Cisco Technical Assistance Center.

Troubleshooting Secure Event Connector Registration Failure

Symptom: Registration of Cisco Secure Event Connector to cloud eventing service fails.

Diagnosis: These are the most common reasons that the SEC fails to register to the eventing cloud service.

- **The SEC is unable to reach the Eventing cloud service from SEC**

  Repair: Ensure that Internet is accessible on port 443 and DNS is configured correctly.

- **Registration failure due to invalid or expired one-time-password in SEC bootstrapdata**

Repair:

Procedure

Step 1   Log on to the SDC as the 'sdc' user.

Step 2   View the connector log: (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) to check registration state.

If registration has failed due to invalid token, you'll see the error message in the log file something similar to the one below.

context:(*contextImpl).handleFailed] registration - CE2001: Registration failed - Failed to register the device because of invalid token. Retry with a new valid token. - Failed"

Step 3   Run the SEC Cleanup Command step on SDC VM to remove the SEC from Secure Connectors page.

Step 4   Generate new SEC bootstrap data and retry the SEC on-boarding steps.

Troubleshooting Network Problems Using Security and Analytics Logging Events

Here is a basic framework you can use to troubleshoot network problems using the Events Viewer.

This scenario assumes that your network operations team has had a report that a user can't access a resource on the network. Based on the user reporting the issue and their location, the network operations team has a reasonable idea of which firewall controls their access to resources.

> **Note**   This scenario also assumes that an FDM-managed device is the firewall managing the network traffic. Security Analytics and Logging does not collect logging information from other device types.

Procedure

Step 1   In the navigation pane, choose **Analytics** > **Event Logging** .

Step 2   Click the **Historical** tab.

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

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

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

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

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

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

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

Troubleshooting NSEL Data Flows

Once you have , use these procedures to verify that NSEL events are being sent from your ASA to the Cisco Cloud and that the Cisco Cloud is receiving them.

Note that once your ASA is configured to send NSEL events to the Secure Event Connector (SEC) and then on to the Cisco Cloud, data does not flow immediately. It could take a few minutes for the first NSEL packets to arrive assuming there is NSEL-related traffic being generated on the ASA.

Note This workflow shows you a straight-forward use of the "flow-export counters" command and "capture" commands to Troubleshoot NSEL Data Flows. See "Packet Captures" CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide and "Monitoring NSEL" in the Cisco ASA NetFlow Implementation Guide for a more detailed discussion of the usage of these commands.

Perform these tasks:

• Verify that NetFlow Packets are Being Sent to the SEC

• Verify that NetFlow Packets are Being Received by the Cisco Cloud

Event Logging Troubleshooting Log Files

The Secure Event Connector (SEC) troubleshoot.sh gathers all event streamer logs and compresses them in a single .tar.gz file.

Use these procedures to create the comparessed .tar.gz file and uncompress the file:

1. Run the Troubleshooting Script, on page 23.

2. Uncompress the sec_troubleshoot.tar.gz file, on page 24.

Run the Troubleshooting Script

The Secure Event Connector (SEC) troubleshoot.sh gathers all event streamer logs and compresses them in a single .tar.gz file. Follow this procedure to run the troubleshoot.sh script:

Procedure

Step 1   Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).

Step 2   Login and then switch to the **root** user:

```
[cdo@localhost ~]$sudo su root
```

Note   You could also switch to the sdc user but acting as root you will also receive IP tables information. The IP table information shows that the firewall is running on the device and all the firewall routes. If the firewall is blocking Secure Event Connector TCP or UDP ports, events will not show up in the Event Logging table. The IP Tables will help you determine if that is the case.

Step 3   At the prompt, run the troubleshoot script and specify the tenant name. This is the command syntax:

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

Here is an example:

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

In the command output, you'll see that the sec_troubleshoot file is stored in the **/tmp/troubleshoot** directory on your SDC. The file name follows the convention **sec_troubleshoot-*timestamp*.tar.gz.**

Step 4   To retrieve the file, log in as the CDO user and download it using SCP or SFTP.

Here is an example:

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

What to do next

Uncompress the sec_troubleshoot.tar.gz file

The Secure Event Connector (SEC) Run the Troubleshooting Script script gathers all event streamer logs and compresses them in a single sec_troubleshoot.tar.gz file. Follow this procedure to uncompress the sec_troubleshoot.tar.gz file.

1.   Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).

2.   Login and then switch to the **root** user:
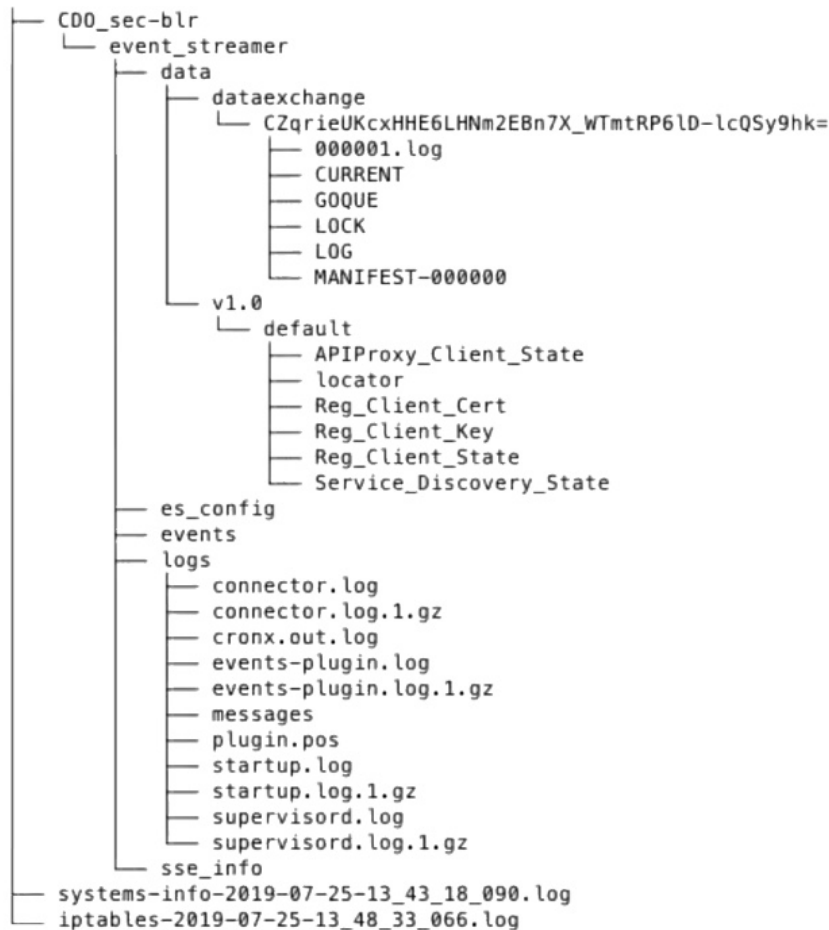
```
[cdo@localhost ~]$sudo su root
```

Note   You could also switch to the **sdc** user but acting as root you will also receive IP tables information. The IP table information shows that the firewall is running on the device and all the firewall routes. If the firewall is blocking Secure Event Connector TCP or UDP ports, events will not show up in the Event Logging table. The IP Tables will help you determine if that is the case.

3.   At the prompt, type the following command:

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

The log files are stored in a directory named after your tenant. These are the kinds of logs stored in the sec_troubelshoot-timestamp.tar.gz file. The iptables file is included if you gathered all the log files as the root user.

```
├── CDO_sec-blr
│   └── event_streamer
│       ├── data
│       │   ├── dataexchange
│       │   │   └── CZqrieUKcxHHE6LHNm2EBn7X_WTmtRP6lD-lcQSy9hk=
│       │   │       ├── 000001.log
│       │   │       ├── CURRENT
│       │   │       ├── GOQUE
│       │   │       ├── LOCK
│       │   │       ├── LOG
│       │   │       └── MANIFEST-000000
│       │   └── v1.0
│       │       └── default
│       │           ├── APIProxy_Client_State
│       │           ├── locator
│       │           ├── Reg_Client_Cert
│       │           ├── Reg_Client_Key
│       │           ├── Reg_Client_State
│       │           └── Service_Discovery_State
│       ├── es_config
│       ├── events
│       ├── logs
│       │   ├── connector.log
│       │   ├── connector.log.1.gz
│       │   ├── cronx.out.log
│       │   ├── events-plugin.log
│       │   ├── events-plugin.log.1.gz
│       │   ├── messages
│       │   ├── plugin.pos
│       │   ├── startup.log
│       │   ├── startup.log.1.gz
│       │   ├── supervisord.log
│       │   └── supervisord.log.1.gz
│       └── sse_info
├── systems-info-2019-07-25-13_43_18_090.log
└── iptables-2019-07-25-13_48_33_066.log
```

Generating SEC Bootstrap data failed.

Symptom: While generating SEC bootstrap data in CDO, the "bootstrap generation" step fails with the error, "There was an error fetching the bootstrap data. Please try again."

Repair: Retry bootstrap data generation again. If it still fails, contact CDO support.

SEC status is "Inactive" in CDO Secure Connectors page after onboarding

Symptom: The Secure Event Connector status shows "Inactive" in the CDO Secure Connectors page for one of these reasons:

- Heartbeat failed

- Connector registration failed

Repair:

- **Heartbeat failed:** Request SEC heartbeat and refresh Secure Connector page to see if the status changes to "Active", if not check if the Secure Device Connector registration failed.

- **Connector registration failed:** Refer issue Troubleshooting Secure Event Connector Registration Failure.

The SEC is "online", but there are no events in CDO Event Logging Page

Symptom: The Secure Event Connector shows "Active" in CDO Secure Connectors page but you do not see events in CDO Event viewer.

Solution or workaround:

Procedure

Step 1   Login to the VM of the on-premise SDC and as the 'sdc' user. At the prompt, type **sudo su - sdc**.

Step 2   Perform these checks:

- Check SEC connector log (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) and ensure the SEC registration was successful. If not, refer issue "Troubleshooting Secure Event Connector Registration Failure".

- Check SEC events log(/usr/local/cdo/data/<tenantDir>/event_streamer/logs/events-plugin.log) and ensure that the events are being processed. If not, contact CDO support.

- Log in to SEC docker container and execute the command "supervisorctl -c /opt/cssp/data/conf/supervisord.conf " and ensure the output is as shown below and all processes in RUNNING state. IIf not, contact CDO support.

estreamer-connector RUNNING pid 36, uptime 5:25:17

estreamer-cron RUNNING pid 39, uptime 5:25:17

estreamer-plugin RUNNING pid 37, uptime 5:25:17

estreamer-rsyslog RUNNING pid 38, uptime 5:25:17

- Ensure that the firewall rules on the on-premise SDC are not blocking the UDP and TCP ports shown for the SEC on the Secure Connectors page. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging to determine what ports you need to open.

- If you have setup SDC manually using a CentOS 7 VM of your own and have the firewall configured to block incoming requests, you could execute the following commands to unblock the UDP and TCP ports:

firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent

firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent

firewall-cmd --reload

- Using Linux network tools of your choice, check if packets are being received on these ports. If not receiving, re-check the FTD logging configuration.

If none of the above repairs work, raise a support ticket with CDO support..

SEC Cleanup Command

The Secure Event Connector (SEC) cleanup command removes the SEC container and it's associated files from the Secure Device Connector (SDC) VM. You might run this command in case of a Troubleshooting Secure Event Connector Registration Failure, on page 21 or onboarding failure.

To run the command:

Before you begin

To perform this task you will need to know the name of your tenant. To locate your tenant name, open the user menu in CDO and click **Settings**. Scroll down the page to locate your **Tenant Name**.

Procedure

Step 1 Log into the SDC as the `sdc` user. At the prompt, type `sudo su - sdc`.

Step 2 Connect to the `/usr/local/cdo/toolkit` directory.

Step 3 Run `sec.sh remove`*tenant_name* and confirm your intent to remove the SEC.

Example:

```
[sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

What to do next

If this command failes to remove the SEC, proceed to SEC Cleanup Command Failure, on page 27

SEC Cleanup Command Failure

Use this procedure if the SEC Cleanup Command, on page 27 failed.

Message: SEC not found, exiting.

Symptom: Cleanup SEC command fails to cleanup existing SEC.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

Repair: Manually cleanup Secure Event Connector when cleanup command fails.

Remove already running SEC docker container:

Procedure

Step 1 Log into the SDC as the `sdc` user. At the prompt, type `sudo su - sdc`.

Step 2 Run **docker ps** command to find the names of the SEC container. The SEC name will be in the format, "es_*name*".

Step 3 Run **docker stop** command to stop the SEC container.

Step 4 Run the **rm** command to remove the SEC container.

For example:

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

Use Health Check to Learn the State of your Secure Event Connector

The Secure Event Connector (SEC) Health Check script provides information on the state of your SEC.

Follow this procedure to run Health Check:

Procedure

Step 1 Open your VM hypervisor and start a console session for your Secure Device Connector (SDC).

Step 2 Login to the SDC as "cdo" user.

Step 3 Switch to the "sdc" user:

```
[cdo@tenant]$sudo su sdc
```

Step 4 At the prompt, run the healthcheck.sh script and specify the tenant name:

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

For example:

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

The output of the script provides this kind of information:

Values of Health Check output:

  • **SEC Cloud URL**: Displays the CDO cloud URL and whether or not the SEC can reach CDO.

- **SEC Connector**: Will show "Running" if the SEC connector has been onboarded correctly and has started.

- **SEC UDP syslog server**: Will show "Running" if the UDP syslog server is ready to send UDP events.

- **SEC TCP syslog server**: Will show "Running" if the TCP syslog server is ready to send TCP events.

- **SEC Connector status**: Will show Active if the SEC is running and onboarded to CDO.

- **SEC Send sample event**: If at the end of the health check, all the status checks are "green," the tool sends a sample event. (If any of the processes are "Down," the tool skips sending the test event.) The sample event shows up in the Event Log as a policy named "sec-health-check."

Troubleshoot Cisco Defense Orchestrator

Troubleshooting Login Failures

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

Make sure you are logging into the appropriate CDO region. After you log into https://sign-on.security.cisco.com, you will be given a choice of what region to access. Click the **CDO** tile to access defenseorchestrator.com or **CDO (EU)** to access defenseorchestrator.eu.

Troubleshooting Login Failures after Migration

Login to CDO Fails Because of Incorrect Username or Password

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

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

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

Login Fails Using a Saved Bookmark

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

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

- **Solution** If you have not yet created a a Cisco Secure Sign-On account, create an account.

- **Solution** If you have created your new account, click the CDO tile on the dashboard that corresponds to Cisco Defense Orchestrator(US), Cisco Defense Orchestrator (EU), or Cisco Defense Orchestrator (APJC)

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

Troubleshooting Access and Certificates

Resolve New Fingerprint Detected State

Procedure

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

Step 2   Click the **Devices** tab.

Step 3   Click the appropriate device type tab.

Step 4   Select the device in the **New Fingerprint Detected** state.

Step 5   Click **Review Fingerprint** in the New Fingerprint Detected pane.

Step 6   When prompted to review and accept the fingerprint:

    a.   Click **Download Fingerprint** and review it.

    b.   If you are satisfied with the fingerprint, click **Accept**. If you are not, click **Cancel**.

Step 7   After you resolve the new fingerprint issue, the connectivity state of the device may show **Online** and the Configuration Status may show "Not Synced" or "Conflict Detected." Review Resolve Configuration Conflicts to review and resolve configuration differences between CDO and the device.

Troubleshooting Network Problems Using Security and Analytics Logging Events

Here is a basic framework you can use to troubleshoot network problems using the Events Viewer.

This scenario assumes that your network operations team has had a report that a user can't access a resource on the network. Based on the user reporting the issue and their location, the network operations team has a reasonable idea of which firewall controls their access to resources.

Note   This scenario also assumes that an FDM-managed device is the firewall managing the network traffic. Security Analytics and Logging does not collect logging information from other device types.

Procedure

Step 1   In the navigation pane, choose **Analytics** > **Event Logging** .

Step 2   Click the **Historical** tab.

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

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

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

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

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

- **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.

- **FirewallPolicy** - The policy in which the rule that triggered the event resides.

- **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.

- **UserName** - The user associated with the initiator IP address. The Initiator IP address is the same as the Source IP address.

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

Troubleshooting SSL Decryption Issues

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

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

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

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

More Details

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

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

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the server. The Alert is usually an "Unknown CA (48)" alert indicating SSL Pinning. A TCP Reset is sent following the Alert message. You should see the following symptoms in the event details:

  - `SSL Flow Flags include ALERT_SEEN.`

  - `SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.`

  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.`

- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is done and then send a TCP Reset. You should see the following symptoms in the event:

  - `SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.`

  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.`

Troubleshoot Intrusion Prevention System

What are my IPS policy options?

Every onboarded device is automatically associated a CDO-provided IPS policy called "Default Overrides". CDO generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. If you want to use the default IPs policy but modify the signature overrides options, see Firepower Intrusion Policy Signature Overrides for more information. Note that configuring different signature overrides per device may cause the default overrides policy to become inconsistent.

How do I have a different IPS policy for every device?

CDO generates a new IPS policy for every FDM-managed device, so there may be multiple policies with this name. You do not have to rename the CDO-provided IPS policy after each device is onboarded. Expanding the policy displays the devices that are associated with it, and you can also filter the threat events page and the signature overrides page per device or policy. To customize the default overrides policy, configure signature overrides per device. This will cause the default overrides intrusions policy to become inconsistent, but this does not inhibit any functionality.

I onboarded a device that has an override configured from FDM.

Overrides that are configured outside of CDO do not pose an issue to device configuration or functionality.

If you onboard a device that has an override already configured and this new device shares an IPs policy with a device that does **not** have an override, the IPS policy will be displayed as **inconsistent**. See Step 3 in Firepower Intrusion Policy Signature Overrides to address inconsistencies.

Troubleshooting Login Failures after Migration

Login to 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.

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

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

Login Fails Using a Saved Bookmark

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

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

- **Solution** If you have not yet created a a Cisco Secure Sign-On account, create an account.

- **Solution** If you have created your new account, click the CDO tile on the dashboard that corresponds to Cisco Defense Orchestrator(US), Cisco Defense Orchestrator (EU), or Cisco Defense Orchestrator (APJC)

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

Troubleshooting Objects

Resolve Duplicate Object Issues

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

To resolve duplicate object issues:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Then filter the objects to find duplicate object issues.

Step 3 Select one of the results. In the objects details panel, you will see the DUPLICATE field with the number of duplicates affected:

⊞ DUPLICATE ②   Resolve | Ignore

Step 4 Click **Resolve**. CDO displays the duplicate objects for you to compare.

Step 5 Select two of the objects to compare.

Step 6 You now have these options:

- If you want to replace one of the objects with the other, click **Pick** for the object you to keep, click **Resolve** to see what devices and network policies will be affected, and then click **Confirm** if you are satisfied with the changes. CDO keeps the object you selected as the replacement and deletes the duplicate.

- If you have an object in the list that you want to ignore, click **Ignore**. If you ignore an object, it will be removed from the list of duplicate objects that CDO shows you.

- Click **Ignore All** if you want to keep the object but do not want CDO to find it in a search for duplicate objects.

Step 7 Once the duplicate object issue has been resolved review and deploy the changes you made now, or wait and deploy multiple changes at once.

Resolving Inconsistent or Unused Security Zone Objects

Security zone objects can be marked inconsistent or unused like other objects. See Resolve Unused Object Issues and Resolve Inconsistent Object Issues for instructions on how to resolve these issues.

Related Information:

- Security Zone Object

- Assign a Firepower Interface to a Security Zone

- Deleting Objects

Resolve Unused Object Issues

Unused objects ⬚ are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule.

Related Information:

- Export a List of Devices and Services

- Bulk Reconnect Devices to CDO

Resolve an Unused Object Issue

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Then filter the objects to find unused object issues.

Step 3 Select one or more unused objects.

Step 4 You now have these options:

- In the Actions pane, click **Remove** 🗑 to remove the unused object from CDO.

- In the Issues pane, click **Ignore.** If you ignore an object, CDO will stop displaying it among the results of unused objects objects.

Step 5 If you removed the unused object, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Note To resolve unused object issues in bulk, see Resolve Object Issues in Bulk.

Remove Unused Objects in Bulk

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2   Then filter the objects to find unused object issues.

Step 3   Select the unused objects you want to delete:

- Click the checkbox in the object table header row to select all the objects on the page.

- Select individual unused objects in the object table.

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

Step 5   Click **OK** to confirm you want to delete the unused objects.

Step 6   You have two choices to deploy these changes:

- Review and deploy the changes you made now, or wait and deploy multiple changes at once.

- Open the **Inventory** page and find the devices that were affected by the change. Select all the devices affected by the change and, in the Management pane, click **Deploy All** ⬆. Read the warning and take the appropriate action.

Resolve Inconsistent Object Issues

Inconsistent objects 🗐 INCONSISTENT ②   Resolve | Ignore   are objects with the same name, but different values, on two or more devices. Sometimes users create objects in different configurations with the same name and content, but over time the values of these objects diverge, which creates the inconsistency.

Note: To resolve inconsistent object issues in bulk, see Resolve Object Issues in Bulk.

You can perform the following on inconsistent objects:

- **Ignore:** CDO ignores the inconsistency between objects and retains their values. The objects will no longer be listed under the inconsistency category.

- **Merge:** CDO combines all selected objects and their values into a single object group.

- **Rename:** CDO allows you to rename one of the inconsistent objects and give it a new name.

- **Convert Shared Network Objects to Overrides:** CDO allows you to combine inconsistent shared objects (with or without overrides) into a single shared object with overrides. The most common default value from the inconsistent objects is set as a default in the newly formed object.

Note   If there are multiple common default values, one of them is selected as the default. The remaining default values and override values are set as overrides of that object.

- **Convert Shared Network Group to Additional Values:** - CDO allows you to combine inconsistent shared network groups into a single shared network group with additional values. The criteria for this functionality is that the inconsistent network groups to be converted must have a minimum of one common object with the same value. All default values that match this criterion becomes the default values, and the remaining objects are assigned as additional values of the newly formed network group.

For example, consider two inconsistent shared network groups. The first network group 'shared_network_group' is formed with 'object_1' (192.0.2.x) and 'object_2' (192.0.2.y). It also contains additional value 'object_3' (192.0.2.a). The second network group 'shared_network_group' is formed with 'object_1' (192.0.2.x) and additional value 'object_4' (192.0.2.b). On converting the shared network group to additional values, the newly formed group 'shared_network_group' contain 'object_1' (192.0.2.x) and 'object_2' (192.0.2.y)' as default values and 'object_3' (192.0.2.a) and 'object_4' (192.0.2.b) as additional values.

> **Note** When you create a new network object, CDO auto assigns its value as an override to an existing shared network object with the same name. This is also applicable when a new device is onboarded to CDO.

The auto-assignment happens only when the following criteria are met:

1. The new network object must be assigned to a device.

2. Only one shared object with the same name and type must be existing in the tenant.

3. The shared object must already contain overrides.

To resolve inconsistent object issues:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Then filter the objects to find inconsistent object issues.

Step 3 Select an inconsistent object. In the objects details panel, you will see the INCONSISTENT field with the number of objects affected:

Step 4 Click **Resolve**. CDO displays inconsistent objects for you to compare.

Step 5 You now have these options:

- **Ignore All:**

  a. Compare the objects presented to you and on one of the objects, click **Ignore**. Or, to ignore all objects, click **Ignore All**.

  b. Click **OK** to confirm.

- **Resolve by merging objects:**

  a. Click **Resolve by Merging X Objects**.

  b. Click **Confirm**.

- **Rename:**

  a. Click **Rename**.

  b. Save your changes to affected network policies and devices and click **Confirm**.

- **Convert to Overrides (for inconsistent shared objects):** When comparing shared objects with overrides, the comparison panel shows only the default values in the **Inconsistent Values** field.

  a. Click **Convert to Overrides**. All inconsistent objects will be converted to a single shared object with overrides.

  b. Click **Confirm**. You can click **Edit Shared Object** to view the details of the newly formed object. You can use up and down arrows to move the values between default and override.

- **Convert to Additional Values (for inconsistent network groups):**

  a. Click **Convert to Additional Values**. All inconsistent objects will be converted to a single shared object with additional values.

  b. Save your changes to affected network policies and devices and click **Confirm**.

Step 6 After resolving the inconsistencies, review and deploy now the changes you made, or wait and deploy multiple changes at once.

Resolve Object Issues in Bulk

One way to resolve objects with Resolve Unused Object Issues, Resolve Duplicate Object Issues, or Resolve Inconsistent Object Issues, on page 35 issues is to ignore them. You can select and ignore multiple objects, even if objects exhibit more than one issue. For example, if an object is both inconsistent and unused, you can only ignore one issue type at a time.

☞

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

To ignore issues in bulk, follow this procedure:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 To narrow your search, you can filter object issues.

Step 3 In the Object table, select all the applicable objects you want to ignore. The Issues pane groups objects by issue type.

Issues	
⊡ Duplicate	Ignore (4)
▣ Inconsistent	Ignore (2)
⸬ Unused	Ignore (1)
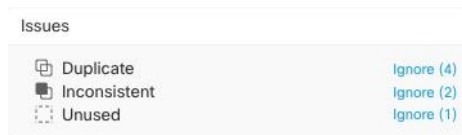
Step 4 Click **Ignore** to ignore issues by type. You must I**gnore** each issue type separately.

Step 5   Click **OK** to confirm you want to ignore those objects.

Device Connectivity States

You can view the connectivity states of the devices onboarded in your CDO tenant. This topic helps you understand the various connectivity states. On the **Inventory** page, the **Connectivity** column displays the device connectivity states.

When the device connectivity state is 'Online' it means that the device is powered on and connected to CDO. The other states described in the table below usually occur when the device is running into problems for various reasons. The table provides the method to recover from such problems. It may be that there is more than one problem causing the connection failure. When you attempt to reconnect, CDO will prompt you to fix all of these problems first before performing the reconnect.

Device Connectivity State	Possible Reasons	Resolution
Online	Device is powered on and connected to CDO.	NA
Offline	Device is powered down or lost network connectivity.	Check whether the device is offline.
Insufficient licenses	Device doesn't have sufficient licenses.	Troubleshoot Insufficient Licenses, on page 40
Invalid credentials	Username and password combination used by CDO to connect to the device is incorrect.	Troubleshoot Invalid Credentials, on page 40
Onboarding	Device onboarding is initiated but is not complete.	Check you device's connectivity and ensure you complete the device registration.
Pending Setup	Device registration has failed.	Troubleshoot Onboarding a Device to the Cloud-delivered Firewall Management Center Using the CLI Registration Key
New Certificate Detected	Certificate on the device has changed. If the device uses a self-signed certificate, then this could have happened due to the device being power cycled.	Troubleshoot New Certificate Issues, on page 41
Device Unregistered	FDM-managed device has been unregistered from Cloud via FDM.	Troubleshoot Device Unregistered, on page 3

Device Connectivity State	Possible Reasons	Resolution
Claim Error	CDO fails to claim the FDM-managed device. Some of the possible reasons could be that an invalid serial number has been entered or the device serial number has already been claimed.	Claim Error
Onboarding Error	CDO may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error, on page 49
Provisioning Error	FDM-managed device initial provisioning has failed.	Provisioning Error
Unreachable	• Device is powered down. • IP address has changed on the device. • Device has been deleted from Cisco Cloud.	Troubleshoot Unreachable Connection State, on page 51

Troubleshoot Device Unregistered

The FDM-managed device may have been unregistered from the cloud via Firewall device manager.

Perform the following to register the device again on the cloud:

Procedure

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the **FTD** tab and select the device in the "Device Unregistered" state, and see the error message on the right.

Step 3 If the unregistered device was onboarded using the registration key, Cisco Defense Orchestrator prompts you to generate a new registration key as the previously applied key has expired.

a) Click the Refresh button to generate a new registration key and then click the Copy icon.

b) Log into the Firewall device manager of the device you want to reregister with CDO.

c) Under **System Settings**, click **Cloud Services**.

d) In the Cisco Defense Orchestrator area, expand **Get Started**.

e) In the **Registration Key** field, paste the registration key that you generated in CDO.

f) Click **Register** and then **Accept** the Cisco Disclosure. Firewall device manager sends the registration request to CDO.

g) Refresh the **Inventory** page in CDO until you see the device's connectivity state changes to "Read Error".

h) Click **Read Configuration** for CDO to read the configuration from the device.

Step 4 If the unregistered device was onboarded using the serial number, CDO prompts you to auto-enroll the device from Firewall device manager.

a) Log into the Firewall device manager of the device you want to reregister with CDO.

b) Under **System Settings**, click **Cloud Services**.

c) Select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click **Register**.

d) Refresh the **Inventory** page in CDO until you see the device's connectivity state changes to "Read Error".

e) Click **Read Configuration** for CDO to read the configuration from the device.

Troubleshoot Insufficient Licenses

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.

- If the device status doesn't change, refresh the CDO portal by signing out from CDO and signing back to resolve any network communication glitch between license server and device.

- If the portal refresh doesn't change the device status, perform the following:

Procedure

Step 1	Generate a new token from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.
Step 2	In the CDO navigation bar, click the **Inventory** page.
Step 3	Click the **Devices** tab.
Step 4	Click the appropriate device type tab and select the device with the **Insufficient License** state.
Step 5	In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.
Step 6	In the **Activate** field, paste the new token and click **Register Device**.
	Once the token is applied successfully to the device, its connectivity state turns to **Online**.

Troubleshoot Invalid Credentials

Perform the following to resolve device disconnection due to invalid credentials:

Procedure

Step 1	Open the **Inventory** page.
Step 2	Click the **Devices** tab.
Step 3	Click the appropriate device type tab and select the device with the **Invalid Credentials** state.
Step 4	In the **Device Details** pane, click **Reconnect** appearing in **Invalid Credentials**. CDO attempts to reconnect with your device.

Step 5   When prompted enter the new username and password for the device.

Step 6   Click **Continue**.

Step 7   After the device is online and ready to use, click **Close**.

Step 8   It is likely that because CDO attempted to use the wrong credentials to connect to the device, the username and password combination CDO should use to connect to the device was changed directly on the device. You may now see that the device is "Online" but the configuration state is "Conflict Detected." Use Resolve Configuration Conflicts to review and resolve configuration differences between CDO and the device.

Troubleshoot New Certificate Issues

CDO's Use of Certificates

CDO checks the validity of certificates when connecting to devices. Specifically, CDO requires that:

1. The device uses a TLS version equal to or greater than 1.0.

2. The certificate presented by the device is not expired, and its issuance date is in the past (i.e. it is already valid, not scheduled to become valid at a later date).

3. The certificate must be a SHA-256 certificate. SHA-1 certificates will not be accepted.

4. One of these conditions is true:

    • The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.

    • The device uses a certificate signed by a trusted Certificate Authority (CA), and provides a certificate chain linking the presented leaf certificate to the relevant CA.

These are the ways CDO uses certificates differently than browsers:

• In the case of self-signed certificates, CDO overrides the domain name check, instead checking that the certificate exactly matches the one trusted by an authorized user during device onboarding or reconnection.

• CDO does not yet support internal CAs. There is currently no way to check a certificate signed by an internal CA.

It is possible to disable certificate checking for ASA devices on a per-device basis. When an ASA's certificate cannot be trusted by CDO, you will have the option of disabling certificate checking for that device. If you have attempted to disable certificate checking for the device and you are still unable to onboard it, it is likely that the IP address and port you specified for the device is incorrect or unreachable. There is no way to disable certificate checking globally, or to disable certificate checking for a device with a supported certificate. There is no way to disable certificate checking for non-ASA devices.

When you disable certificate checking for a device, CDO will still use TLS to connect to the device, but it will not validate the certificate used to establish the connection. This means that a passive man-in-the-middle attacker will not be able to eavesdrop on the connection, but an active man-in-the-middle could intercept the connection by supplying CDO with an invalid certificate.

Identifying Certificate Issues

There are several reasons that CDO may not be able to onboard a device. When the UI shows a message that "CDO cannot connect to the device using the certificate presented," there is a problem with the certificate. When the UI does not show this message, the problem is more likely related to connectivity problems (the device is unreachable) or other network errors.

To determine why CDO rejects a given certificate, you can use the openssl command-line tool on the SDC host or another host that can reach the relevant device. Use the following command to create a file showing the certificates presented by the device:

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

This command will start an interactive session, so you will need to use Ctrl-c to exit after a couple of seconds.

You should now have a file containing output like the following:

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
```

```
     Protocol : TLSv1.2
     Cipher : ECDHE-RSA-AES128-GCM-SHA256
     Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
     Session-ID-ctx:
     Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

     Key-Arg : None
     PSK identity: None
     PSK identity hint: None
     SRP username: None
     TLS session ticket lifetime hint: 100800 (seconds)
     TLS session ticket:
     0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de   z.T..H~v0s...@[.
     0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c   .S..A6f>[5...o}.
     0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6   K..o....1[..eo..
     0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28   q=.S.)A.......3(
     0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36   ..n....c...c.d.6
     0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d   "..:Y...\!..R(E.
     0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d   r..#...|....+.B.
     0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de   #5m.}.9...I.....
     0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45   ...^E.|.k.x.I..E
     0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63   n.$.E.A....J.6.c
     00a0 - 72 a4 ad                                          r..
     00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

The first thing to note in this output is the last line, where you see the **Verify return code**. If there is a certificate issue, the return code will be non-zero and there will be a description of the error.

Expand this list of certificate error code to see common errors and how to remediate them

0 X509_V_OK The operation was successful.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT The issuer certificate of an untrusted certificate could not be found.

3 X509_V_ERR_UNABLE_TO_GET_CRL The CRL of a certificate could not be found.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. This is only meaningful for RSA keys.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE The CRL signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. Unused.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY The public key in the certificate SubjectPublicKeyInfo could not be read.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE The signature of the certificate is invalid.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE The signature of the certificate is invalid.

9 X509_V_ERR_CERT_NOT_YET_VALID The certificate is not yet valid: the notBefore date is after the current time. See Verify return code: 9 (certificate is not yet valid) below for more information.

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired; that is, the notAfter date is before the current time. See Verify return code: 10 (certificate has expired) below for more information.

11 X509_V_ERR_CRL_NOT_YET_VALID The CRL is not yet valid.

12 X509_V_ERR_CRL_HAS_EXPIRED The CRL has expired.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD The certificate notBefore field contains an invalid time.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD The certificate notAfter field contains an invalid time.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD The CRL lastUpdate field contains an invalid time.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD The CRL nextUpdate field contains an invalid time.

17 X509_V_ERR_OUT_OF_MEM An error occurred trying to allocate memory. This should never happen.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN The certificate chain could be built up using the untrusted certificates but the root could not be found locally.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE No signatures could be verified because the chain contains only one certificate and it is not self-signed. See "Verify return code: 21 (unable to verify the first certificate)" below for more information. Verify return code: 21 (unable to verify the first certificate) below for more information.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG The certificate chain length is greater than the supplied maximum depth. Unused.

23 X509_V_ERR_CERT_REVOKED The certificate has been revoked.

24 X509_V_ERR_INVALID_CA A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED The basicConstraints pathlength parameter has been exceeded.

26 X509_V_ERR_INVALID_PURPOSE The supplied certificate cannot be used for the specified purpose.

27 X509_V_ERR_CERT_UNTRUSTED The root CA is not marked as trusted for the specified purpose.

28 X509_V_ERR_CERT_REJECTED The root CA is marked to reject the specified purpose.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.

30 X509_V_ERR_AKID_SKID_MISMATCH The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH The current candidate issuer certificate was rejected because its issuer name and serial number were present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.

50 X509_V_ERR_APPLICATION_VERIFICATION An application specific error. Unused.

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, CDO may generate a "New Certificate Detected" message as both a **Configuration Status** and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from CDO. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Note   When you bulk reconnect more than one managed device to CDO at the same time, CDO automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Use the following procedure to resolve a new certificate:

1. Navigate to the **Inventory** page.

2. Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.

3. In the action pane, click **Review Certificate**. CDO allows you to download the certificate for review and accept the new certificate.

4. In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

    CDO automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the **Inventory** page to see the device once it's synched.

Certificate Error Codes

Verify return code: 0 (ok) but CDO returns certificate error

Once CDO has the certificate, it attempts to connect to the URL of the device by making a GET call to "https://<device_ip>:<port>". If this does not work, CDO will display a certificate error. If you find that the certificate is valid (openssl returns 0 ok) the problem may be that a different service is listening on the port you're trying to connect to. You can use the command:

```
 curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

to determine whether you are definitely talking to an ASA and check if HTTPS server running on the correct port on the ASA:

```
 # show asp table socket
Protocol        Socket        State        Local Address          Foreign Address
SSL             00019b98      LISTEN         192.168.1.5:443          0.0.0.0:*
SSL             00029e18      LISTEN         192.168.2.5:443          0.0.0.0:*
TCP             00032208      LISTEN         192.168.1.5:22           0.0.0.0:*
```

Verify return code: 9 (certificate is not yet valid)

This error means that the issuance date of the certificate provided is in the future, so clients will not treat it as valid. This can be caused by a poorly-constructed certificate, or in the case of a self-signed certificate it can be cause by the device time being wrong when it generated the certificate.

You should see a line in the error including the notBefore date of the certificate:

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
```

```
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

From this error, you can determine when the certificate will become valid.

Remediation

The notBefore date of the certificate needs to be in the past. You can reissue the certificate with an earlier notBefore date. This issue can also arise when the time is not set correctly either on the client or issuing device.

Verify return code: 10 (certificate has expired)

This error means that at least one of the certificates provided has expired. You should see a line in the error including the notBefore date of the certificate:

```
 error 10 at 0 depth lookup:certificate has expired
```

The expiration date is located in the certificate body.

Remediation

If the certificate is truly expired, the only remediation is to get another certificate. If the certificate's expiration is still in the future, but openssl claims that it is expired, check the time and date on your computer. For instance, if a certificate is set to expire in the year 2020, but the date on your computer is in 2021, your computer will treat that certificate as expired.

Verify return code: 21 (unable to verify the first certificate)

This error indicates that there is a problem with the certificate chain, and openssl cannot verify that the certificate presented by the device should be trusted. Let's look at the certificate chain from the example above to see how certificate chains should work:

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

The certificate chain is a list of certificates presented by the server, beginning with the server's own certificate and then including increasingly higher-level intermediate certificates linking the server's certificate with a Certificate Authority's top-level certificate. Each certificate lists its Subject (the line starting with 's:' and its Issuer (the line starting with 'i').

The Subject is the entity identified by the certificate. It includes the Organization name and sometimes the Common Name of the entity for which the certificate was issued.

The Issuer is the entity that issued the certificate. It also includes an Organization field and sometimes a Common Name.

If a server had a certificate issued directly by a trusted Certificate Authority, it would not need to include any other certificates in its certificate chain. It would present one certificate that looked like:

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

Given this certificate, openssl would verify that the ExampleCo certificate for ***.example.com** was correctly signed by the Trusted Authority certificate, which would be present in openssl's built-in trust store. After that verification, openssl would successfully connect to the device.

However, most servers do not have certificates signed directly by a trusted CA. Instead, as in the first example, the server's certificate is signed by one or more intermediates, and the highest-level intermediate has a certificate signed by the trusted CA. OpenSSL does not trust these intermediate CAs by default, and can only verify them if it is given a complete certificate chain ending in a trusted CA.

It is critically important that servers whose certificates are signed by intermediate authorities supply ALL the certificates linking them to a trusted CA, including all of the intermediate certificates. If they don't supply this entire chain, the output from openssl will look something like this:

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
```

```
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

This output shows that the server only provided one certificate, and the provided certificate was signed by an intermediate authority, not a trusted root. The output also shows the characteristic verification errors.

Remediation

This problem is caused by a misconfigured certificate presented by the device. The only way to fix this so that CDO or any other program can securely connect to the device is to load the correct certificate chain onto the device, so that it will present a complete certificate chain to connecting clients.

To include the intermediate CA to the trustpoint follow one of the links below (depending on your case - if CSR was generated on the ASA or not):

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, CDO may generate a "New Certificate Detected" message as both a **Configuration Status** and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from CDO. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Note   When you Bulk Reconnect Devices to CDO more than one managed device to CDO at the same time, CDO automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Use the following procedure to resolve a new certificate:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.

Step 5 In the action pane, click **Review Certificate**. CDO allows you to download the certificate for review and accept the new certificate.

Step 6 In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

CDO automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the **Inventory** page to see the device once it's synched.

Troubleshoot Onboarding Error

The device onboarding error can occur for various reasons.

You can take the following actions:

Procedure

Step 1 On the **Inventory** page, click the **Devices** tab.

Step 2 Click the appropriate device type tab and select the device running into this error. In some cases, you will see the error description on the right. Take the necessary actions mentioned in the description.

Or

Step 3 Remove the device instance from CDO and try onboarding the device again.

Resolve the Conflict Detected Status

CDO allows you to enable or disable conflict detection on each live device. If Conflict Detection is enabled and there was a change made to the device's configuration without using CDO, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Procedure

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

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Conflict Detected** state and continue from Step 4.

Step 2	Click the **Devices** tab to locate your device.
Step 3	Click the appropriate device type tab.
Step 4	Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.
Step 5	In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

> • The panel labeled "Last Known Device Configuration" is the device configuration stored on CDO.
>
> • The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

Step 6	Resolve the conflict by selecting one of the following:

> • **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on CDO** with the device's running configuration.
>
> > **Note**   As CDO does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.
>
> • **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on CDO.
>
> **Note**   All configuration changes, rejected or accepted, are recorded in the change log.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Procedure

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

> **Note**   For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 2	Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
Step 3	Click the appropriate device type tab.
Step 4	Select the device reported as Not Synced.
Step 5	In the **Not synced** panel to the right, select either of the following:

> • **Preview and Deploy...** -If you want to push the configuration change from CDO to the device, preview and deploy the changes you made now, or wait and deploy multiple changes at once.

- **Discard Changes** -If you do **not** want to push the configuration change from CDO to the device, or you want to "undo" the configuration changes you started making on CDO. This option overwrites the configuration stored in CDO with the running configuration stored on the device.

Troubleshoot Unreachable Connection State

The device may be in "unreachable" for various reasons:

Procedure

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

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

Step 3   Click the appropriate device type tab and select the device in the **Unreachable** state.

Step 4   Click ⚡ **Reconnect.**

Step 5   Take one of these actions based on the message appearing on the right:

    a. If you have onboarded the FDM-managed device using the IP address and device credentials, the following message appears:

    "*This device is unreachable, review the IP address and port*," enter the new IP address and/or new port information of the device in the message box. It is likely that because CDO attempted to connect to an invalid IP address, the IP address for the device was changed directly on the device.

| **Note** | If the device was rebooted, and there are no other pending changes, the device should return to an online connection state, and no further action is needed. |

    You may now see that the device is "Online", but the configuration state is "Conflict Detected." Use Resolve Configuration Conflicts, to review the configuration differences between CDO and the device.

    b. If you are onboarding the FDM-managed device using the registration token or serial number, the following message appears:

    "*This device has been deleted from Cisco Cloud. The deletion could be caused as part of the Return Material Authorization (RMA) process*". It means that the faulty device that you have returned to the RMA team has been deleted from Cisco Cloud as a part of the RMA process.

    As a result, you'll see that the device Connectivity status is "Unreachable" in CDO.

      - For the RMA case, you need to perform the following steps in CDO:

        1. If the device was successfully onboarded, you need to save the device configuration as a template. See Configure an FDM Template.

        Remove the device instance from CDO.

        2. Power on the new replacement device that you have received from the RMA team and onboard it to CDO. See Onboard an FDM-Managed Device using the Device Serial Number.

| **Important** | The replacement device will probably have a different serial number and needs to be onboarded as a new device. |

You'll now see that the device is "Online", but the configuration state is "Conflict Detected."

3. Use Resolve Configuration Conflicts, to review the configuration differences between CDO and the device.

Apply the previously saved template to the new device. See Apply an FDM Template.

- If you have sold the device or transferred its ownership to another user outside of your tenant without erasing the device's configuration, you will no longer possess the device. This error occurs when the buyer reimages the device. If the device was configured correctly and synced earlier, you can save the device configuration as a template and then remove the device instance from CDO.