

Troubleshooting

This chapter details how to troubleshoot errors that may occur when working with various components in Security Cloud Control Firewall Management.

- Troubleshoot a Secure Firewall ASA device, on page 1
- Troubleshoot a Secure Device Connector, on page 11
- Troubleshoot a Secure Event Connector, on page 20
- Troubleshoot Security Cloud Control, on page 27
- Device connectivity states, on page 31

Troubleshoot a Secure Firewall ASA device

ASA Fails to Reconnect to Security Cloud Control After Reboot

If Security Cloud Control and your ASA do not connect after an ASA reboot, it may be because the ASA has fallen back to using an OpenSSL cipher suite that is not supported by Security Cloud Control's Secure Device Connector (SDC). This troubleshooting topic tests for that case and provides remediation steps.

Symptoms

- ASA reboots and Security Cloud Control and the ASA fail to reconnect. Security Cloud Control displays the message, "Failed to reconnect."
- When attempting to onboard an ASA, Security Cloud Control displays the message: *Certificate could not be retrieved for <ASA_IP_Address>*.

Cannot onboard ASA due to certificate error

Environment: ASA is configured with client-side certificate authentication.

Solution: Disable client-side certificate authentication.

Details: ASAs support credential-based authentication as well as client-side certificate authentication. Security Cloud Control cannot connect to ASAs that use client-side certificate authentication. Before onboarding your ASA to Security Cloud Control, make sure it does not have client-certificate authentication enabled by using this procedure:

Procedure

Step 1 Open a terminal window and connect to the ASA using SSH.

Step 2 Enter global configuration mode.

Step 3 At the hostname (config)# prompt, enter this command:

```
no ssl certificate-authentication interface interface-name port 443
```

The interface name is the name of the interface Security Cloud Control connects to.

Determine the OpenSSL Cipher Suite Used by your ASA

Use this procedure to identify the OpenSSL cipher suite being used by your ASA. If the cipher suite named in the command output is not in the list of supported cipher suites, the SDC doesn't support that cipher suite and you will need to update the cipher suites on your ASA.

Procedure

Step 1 Open a console window on a computer that can reach the SDC.

Step 2 Connect to your SDC using SSH. You can log in as a regular user such as Security Cloud Control or SDC or some other user you created. You don't need to be logged in as root.

Tip
To find your SDC IP address:

a. Open Security Cloud Control.

b. From the user menu, select Secure Device Connectors.

c. Click the SDC displayed in the table. The IP address of the SDC is displayed in the details pane for the device.

Step 3 At the command prompt enter: **openssl s_client -showcerts -connect** *ASA_IP_Address*:**443**

Step 4 Look for these lines in the command output.

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

In this example, the cipher suite being used by the ASA is `DES-CB3-SHA`.

Cipher Suites Supported by Security Cloud Control's Secure Device Connector

Security Cloud Control's Secure Device Connector uses node.js which only accepts the latest and most secure ciphers. As a result, Security Cloud Control's SDC only supports this list of ciphers:

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

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

Updating your ASA's Cipher Suite

To update the TLS cipher suites on an ASA:

Procedure

Step 1 Connect to the ASA using SSH.

Step 2 Once connected to the ASA, elevate your privileges to global configuration mode. Your prompt should look like this: asaname(config)#

Step 3 At the prompt, enter a command similar to this:

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384
 ECDHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA256"
```

Note
The cipher suites this command configures your ASA to support are contained between quotes and after the word custom. In this command, the cipher suites specified begin with `ECDHE-RSA-AES128-GCM-SHA256` and end with `DHE-RSA-AES256-SHA256`. When you enter the command on your ASA, remove any cipher suites you know your ASA will not support.

Step 4 After you submit the command, enter write memory at the prompt to save the local configuration. For example:

```
asaname(config)#write memory
```

Troubleshoot ASA using CLI commands

This section discusses some of the important commands you may want to use to troubleshoot the ASA and test basic connectivity. See CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide to learn about other troubleshooting scenarios and CLI commands. In the 'System Administration' section, navigate to the 'Testing and Troubleshooting' chapter.

You can use the Security Cloud Control CLI interface available for each ASA device to execute these commands.

See ASA command line interface to learn about how to use the CLI interface in Security Cloud Control.

NAT Policy Settings

Some of the important commands to determine the NAT settings are as follows:

- To determine NAT policy statistics, use **show nat**.
- To determine the NAT pools, including the addresses and ports allocated, and how many times they were allocated, use **show nat pool**.

For more commands related to NAT, see CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, and navigate to the 'Network Address Translation (NAT)' chapter.

Test Basic Connectivity: Pinging Addresses

You can ping the ASA device using the **ping <IP address>** command using the ASA CLI interface. To learn about

Display the Routing Table

Use the **show route** command to view the entries in the routing table.

ciscoasa# show route

Example output for a routing table of an ASA:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, + - replicated route

SI - Static InterVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management

C 10.0.0.0 255.0.0.0 is directly connected, Outside

L 10.10.10.1 255.255.255.255 is directly connected, Outside
```

```
C 192.168.0.0 255.255.255.0 is directly connected, management

L 192.168.0.118 255.255.255.255 is directly connected, management
```

Monitor Switch Ports

- **show interface**

  Displays interface statistics.

- **show interface ip brief**

  Displays interface IP addresses and status.

- **show arp**

Shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds.

Example output of ARP entries:

```
management 10.10.32.129 0050.568a.977b 0

management 10.10.32.136 0050.568a.5387 21

LANFAIL 20.20.21.1 0050.568a.4d70 96

outsi 10.10.16.6 0050.568a.e6d3 3881

outsi 10.10.16.1 0050.568a.977b 5551
```

Troubleshoot ASA Remote Access VPN

This section discusses some of the troubleshooting issues that may occur when configuring remote access VPN on an ASA device.

Missing Information on the RA VPN Monitoring Page

This issue may occur if the outside interface is not enabled for Webvpn.

Resolution:

1. In the navigation pane, click **Inventory**.
2. Click the **Devices** tab and then click the **ASA** tab.
3. In the left pane, click **Security Devices** and then click the **ASA** tab.
4. Select the RA VPN headend ASA device that is having issues.
5. In the **Management** pane on the right, click **Configuration**.
6. Click **Edit** and search for ‘webvpn’.
7. Press **Enter** and add `enable` *interface_name*. Here, the interface_name is the name of the outside interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile.

   For example:

```
webvpn

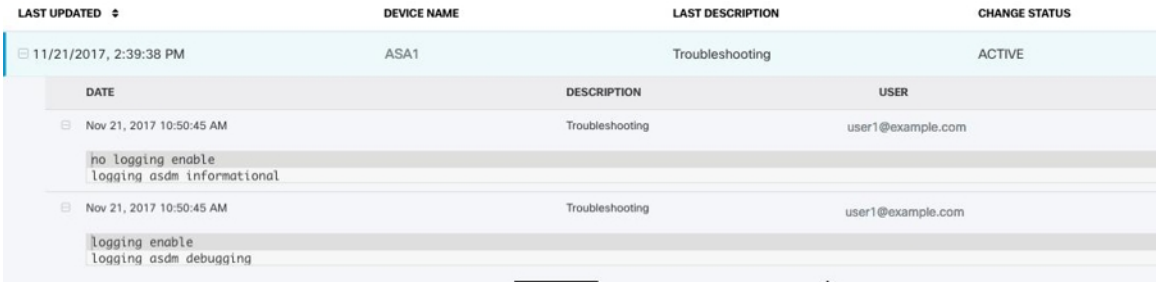
enable outside
```

8. Click **Save**.
9. Preview and deploy the configuration to the device.

ASA Real-time Logging

Use real-time logging to display the last 20 seconds of logged data or the last 10 KB of logged data, whichever limit is reached first. When Security Cloud Control retrieves the real-time data, it reviews the existing logging configuration on your ASDM, changes it to request debugging-level data, and then returns the logging configuration to your configuration. The logging Security Cloud Control displays reflects any logging filters you may have set in ASDM.

You can see the commands that Security Cloud Control sends to perform logging by reviewing the change log. Below is an example of a change log entry. The first entry (on the bottom) indicates that Security Cloud Control "turned on" logging with the logging enable command and changed the ASDM logging level to debugging. The second entry (on the top) shows that the logging configuration was returned to its previous state. Logging was "turned off" with the no logging enable command and the ASDM logging level was returned to informational.



View ASA Real-time Logs

Procedure

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

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the appropriate device type tab and select the device for which you want to view real-time data.

Step 4 Click **Troubleshoot** Troubleshoot.

Step 5 (Optional) Before clicking View Real-time Log, you can define a filter in the left pane to refine the results of your logging search.

Step 6 Click **View Real-time Log**. Security Cloud Control retrieves the real-time logging data based on your filterin criteria and displays it.

Step 7 To see an additional 20 seconds of logged data or the last 10 KB of logged data. click **View Real-Time Log** again.

ASA Packet Tracer

Packet tracer allows you to send a synthetic packet into the network and evaluate how the existing routing configuration, NAT rules, and policy configurations, affect that packet. Use this tool to troubleshoot these kinds of issues:

- Users report that they cannot reach resources that they should be able to.
- Users report that they can reach resources they should not be able to.
- Test a policy to determine if it works as you expect.

Packet tracer can be used on a live, online, ASA device either physical or virtual. Packet Tracer does not work on ASA model devices. Packet tracer evaluates packets based on the saved configuration on the ASA. Staged changes on Security Cloud Control are not evaluated by packet tracer.

We consider it a best-practice to run packet tracer on an ASA that is in the synced state. Though packet tracer will run if the device is not synced, you could encounter some unexpected results. For example, if you deleted a rule in the staged configuration on Security Cloud Control, and this same rule was triggered on the ASA during packet tracing, Security Cloud Control won't be able to show you the result of the packet's interaction with that rule.

Troubleshooting with ASA Packet Tracer

As packet tracer sends the packet through the routing configuration, NAT rules, and security policies of your ASA, it displays the packet's status at each step. If the packet is allowed by the policy it receives a green checkmark. If a packet is denied and dropped, Security Cloud Control displays a red X.

Packet tracer also displays a real time log of the result of the packet trace. In the example below, you can see where a rule denied a tcp packet.



Troubleshoot an ASA Device Security Policy

Procedure

Step 1 From the **Inventory** page, select your ASA, and click **Troubleshoot** Troubleshoot in the Actions pane.

Step 2 In the left pane, click **Security Devices**.

Step 3 Select your ASA and view troubleshooting details in the **Troubleshooting** pane.

Step 4 In the pane, select the interface and packet type you want to send virtually through your ASA.

Step 5 (Optional) If you want to trace a packet where the security group tag value is embedded in the Layer 2 CMD header (Trustsec), check SGT number and enter the security group tag number, 0-65535.

Step 6 Specify the source and destination. You can specify IPv4 or IPv6 addresses, fully-qualified domain names (FQDN), or security group names or tags if you use Cisco Trustsec. For the source address, you can also specify a username in the format Domain\username.

Step 7 Specify other protocol characteristics:

- ICMP-Enter the ICMP type, ICMP code (0-255), and optionally, the ICMP identifier.
- TCP/UDP/SCTP-Enter the source and destination ports by selecting them from the list or entering a value in the port combo box.
- IP-Enter the protocol number, 0-255.

Step 8 Click **Run Packet Tracer**.

Step 9 Continue with Analyze Packet Tracer Results.

Troubleshoot an Access Rule

Procedure

Step 1 Select **Policies** > **Network Policies**.

Step 2 In the left pane, click **Policies** > **ASA** > **Access Policies**.

Step 3 Select a policy that is associated with your ASA.

Step 4 Select a rule in the network policy to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. Notice that in the values panel of the troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.

Step 5 Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer button becomes active.

Step 6 Click **Run Packet Tracer.**

Step 7 Continue with Analyze Packet Tracer Results.

Troubleshoot a NAT Rule

Procedure

Step 1 From the **Inventory** page, select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.

Step 2 In the left pane, click **Security Devices** and then click the **ASA** tab.

Step 3 Select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.

Step 4 Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. Notice that in the values panel of the Troubleshoot page, many of the fields are pre-populated with the attributes of the rule you chose.

Step 5 Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.

Step 6 Click **Run Packet Tracer.**

Step 7 Continue with Analyze Packet Tracer Results.

Troubleshoot a Twice NAT Rule

Procedure

Step 1 From the **Inventory** page, select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.

Step 2 In left pane, click **Security Devices**.

Step 3 Click the **ASA** tab, select your ASA, and click **View NAT Rules** View NAT Rules in the Action pane.

Step 4 Select the rule from the NAT Rules table that you want to troubleshoot and click **Troubleshoot** Troubleshoot in the details pane. For a bi-directional Twice NAT rule, this opens a dropdown where you choose to troubleshoot the source packet translation or the destination packet translation.

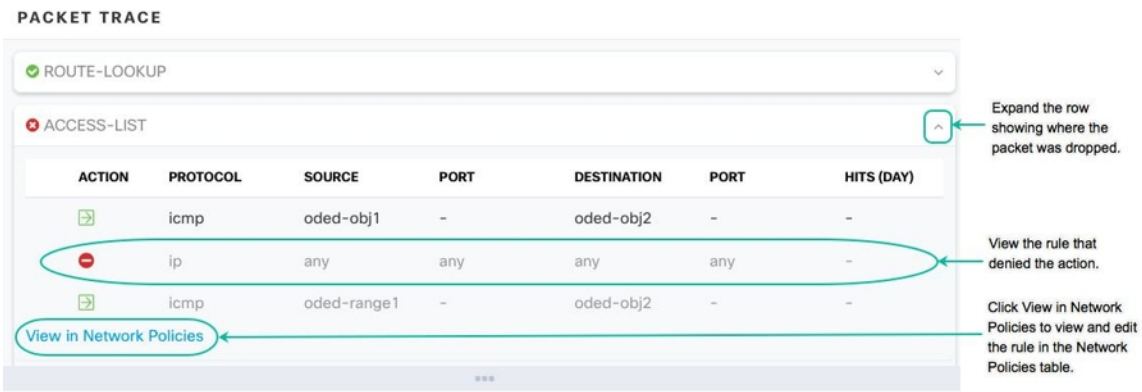
Step 5 Enter information in the remaining required fields. Once you have completed all the required fields the Run Packet Tracer becomes active.

Step 6 Click **Run Packet Tracer**.

Analyze Packet Tracer Results

Whether the packet is dropped or allowed, you can learn why by expanding a row in the packet trace table and reading the rule or logging information related to that action. In the example below, packet tracer identified an access list policy that included a rule to deny an IP packet coming from any source and going to any destination. If this is not the action you want, you can click the **View in Network Policies** link and edit that rule immediately. After you edit the rule, be sure to deploy that configuration change to the ASA and then re-run packet tracer to ensure that you get the access results you expect.

Along with the packet tracer results, Security Cloud Control displays the real-time logs from the ASA.



Confirming ASA Running Configuration Size

To confirm the size of your running configuration file, follow this procedure:

Procedure

Step 1 Access the ASA's command line interface in one of these ways:

- Open a terminal window and log into your ASA using SSH. Elevate your privilege to "privileged EXEC" mode so you see the prompt with `hostname#` .
- If you managed to get your ASA onboarded, open the **Security Devices** page, select the device you want to connect to, and click **>_ Command Line Interface** button in the Device Actions pane.

Step 2 At the prompt type `copy running-config flash`

Step 3 When prompted for the Source filename, don't type anything and press <Enter>

Step 4 When prompted for the destination filename, enter a name for the output file. After ASA copies the running configuration the file you specified, it returns you to the privileged EXEC prompt.

Step 5 At the prompt, type `show flash`

Step 6 Look in the length column. If your file is over 4718592 bytes, it is larger than 4.5 MB.

Here is a sample set of commands and output:

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

Large ASA Running Configuration Files

Behavior in Security Cloud Control

You may see behavior such as the ASA failing to onboard, Security Cloud Control not displaying all of the configuration defined in the ASA's running configuration file, or Security Cloud Control failing to write to the change log.

Possible Cause

The running configuration file of your ASA may be "too large" for Security Cloud Control.

When you an onboard an ASA to Security Cloud Control, Security Cloud Control stores a copy of the ASA's running configuration file in its database. Generally, if that running configuration file is too large (4.5 MB or larger), or it contains too many lines (approximately 22,000 lines), or there are too many access-list entries for a single access group, Security Cloud Control will not be able to predictably manage that device.

To confirm the size of your running configuration file, see Confirming ASA Running Configuration Size.

Workaround or Solution

Contact your Cisco account team for help safely reducing the size of your configuration file without disrupting your security policies.

Troubleshoot a Secure Device Connector

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

If none of these scenarios match yours, 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 Security Cloud Control in a row. If your SDC is unreachable, your tenant will not be able to communicate with any of the devices you have onboarded.

Security Cloud Control 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 Security Cloud Control 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 Security Cloud Control IP address in your region.
2. Attempt to reconnect Security Cloud Control and the SDC by requesting a heartbeat manually. If the SDC responds to a heartbeat request, it will return to "Active" status. To request a heartbeat manually:
   a. In the left pane, choose **Administration** > **Integrations** > **Secure Connectors**.
   b. Click the SDC that is unreachable.
   c. In the Actions pane, click **Request Heartbeat**.
   d. Click **Reconnect**.
3. If the SDC does not return to the Active status after manually attempting to reconnect it to your tenant, follow the instructions in SDC Status not Active on Security Cloud Control After Deployment, on page 11.

.

SDC Status not Active on Security Cloud Control After Deployment

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

Procedure

Step 1 In Security Cloud Control, click on the SDC that isn't showing as active, and click **Request Heartbeat**.

Step 2 Ensure that the container is running using the command:

```
docker ps
```

Step 3 View the SDC logs and check for errors using the command:

```
sdc show logs
```

Step 4 Restart the container using the command:

```
sdc restart
```

Changed IP Address of the SDC is not Reflected in Security Cloud Control

To view the updated IP address of an SDC, request a heartbeat using the steps provided earlier, and then refresh your browser.

Request a Heartbeat

In Security Cloud Control, click on the SDC that isn't showing as active, and, in the sidebar, click **Request Heartbeat**.

1. Make sure the container is running using the command: `docker ps`
2. View the SDC logs and check for errors using the command `sdc show logs`
3. Restart the container using the command `sdc restart`

Troubleshoot Device Connectivity with the SDC

Use this tool to test connectivity from Security Cloud Control, 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 Security Cloud Control can reach your device.

Procedure

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

Step 2 In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**, and click the **Secure Connectors** tab.

Step 3 Select the SDC.

Step 4 In the **Troubleshooting** pane on the right, click **Device Connectivity**.

Step 5 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**. Security Cloud Control 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, Security Cloud Control 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 6 If you continue to have issues onboarding or connecting to the device, contact Security Cloud Control support.

Intermittent or No Connectivity with SDC

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies only to an on-premise SDC and if you are still using CentOS.

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 Security Cloud Control and click **Request Reconnect** from the Actions menu.
7. Before your SDC status can change from Unreachable to Active, you must go to the **Secure Connectors** tab which you can navigate to from **Administration** > **Integrations** > **Firewall Management Center** 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 Security Cloud Control customers:

- Customers using Security Cloud Control's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the Security Cloud Control 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 Security Cloud Control-Standard SDC Host, on page 15
  - Updating a Custom SDC Host, on page 15
  - Bug Tracking, on page 16

Updating a Security Cloud Control-Standard SDC Host

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 Security Cloud Control 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

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- 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

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control 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, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

- Security Cloud Control'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.

Follow the steps below to correct the system time issue. Once this problem is resolved, you can 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 Security Cloud Control 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.

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 Security Cloud Control operations team can complete your SDC migration to the new communication method.

SDC version is lower than 202311****

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control 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, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

- Security Cloud Control'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 Security Cloud Control navigation menu, **Administration** > **Integrations** > **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, Security Cloud Control operations will 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`. Security Cloud Control 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 Security Cloud Control.

b) Navigate to the Secure Connectors page by navigating from the Security Cloud Control 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.

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 Security Cloud Control operations team can run the migration process again.

Certificate or Connection errors with AWS servers

Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control 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, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

Security Cloud Control'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 Australia region:
  - cognito-identity.ap-southeast-2.amazonaws.com
  - cognito-idp.ap-southeast-2.amazonaws.com
  - sns.ap-southeast-2.amazonaws.com
  - sqs.ap-southeast-2.amazonaws.com

- Production tenants in the India region:
  - cognito-identity.ap-south-1.amazonaws.com
  - cognito-idp.ap-south-1.amazonaws.com
  - sns.ap-south-1.amazonaws.com
  - sqs.ap-south-1.amazonaws.com
- Production tenants in the US region:
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- Production tenants in the EU region:
  - cognito-identity.eu-central-1.amazonaws.com
  - cognito-idp.eu-central-1.amazonaws.com
  - sns.eu-central-1.amazonaws.com
  - sqs.eu-central-1.amazonaws.com
- Production tenants in the APJ region:
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

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

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

- Production tenants in the US region:

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

- Production tenants in the EU region:

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

- Production tenants in the APJ region:

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

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

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

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 Security Cloud Control operations team can complete your SDC migration to the new communication method.

Troubleshoot a Secure Event Connector

If none of the scenarios described below match your issue, open a case with Cisco Technical Assistance Center (TAC) for further assistance.

Troubleshoot SEC Onboarding Failures

The troubleshooting scenarios describe a variety of symptoms associated with Secure Event Connector (SEC) onboarding and operational failures. Use this topic to identify and resolve the issue impacting your deployment.

SEC onboarding failed

Symptom: SEC onboarding failed.

Repair: Remove and onboard the SEC again.

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, gather the troubleshooting logs and contact your Managed Service Provider or the Cisco Technical Assistance Center.

Downloading, decoding, or extracting bootstrap data failed

Messages:

- `[Error] Downloading the bootstrap package failed.`
- `[Error] Extracting the bootstrap package failed.`
- `[Error] Max retries exceeded for bootstrap download.`

Diagnosis: Decoding bootstrap data failed.

Repair:

- Wait briefly and retry the bootstrap operation.

- Add a new SEC in the UI and attempt to bootstrap the new one instead.

Adequate CPU and memory not available

Message: [Error] Secure Event Connector minimum system requirements not met.

```
 [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: Increase the resources of your virtual machine to meet the minimum required specifications.

Host already has an SEC

Message: [Error] This host currently has an SEC enabled for the same tenant. Please remove the SEC before trying to bootstrap it again.

Diagnosis: SEC already running.

Repair: Ensure that there is no existing operational SEC in your environment. If one is present but not operational, remove it and then re-bootstrap the SEC.



Note Ensure that you are removing an active SEC. This error message can occur when a bootstrap progresses far enough for the system to assume normal operation but fails to fully complete. As a result, it is possible that a bootstrap error is causing this situation.

To confirm, run the command `sdc eventing healthcheck`. If the health check reports all green, it indicates that the SEC is active and functioning properly. In such a case, removing it would disrupt an operational SEC.

Contact Security Cloud Control Support

If none of the scenarios described above match your issue, open a case with Cisco Technical Assistance Center.

Troubleshoot 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 SSH to the host VM as the admin user, typically `cdo`.

Step 2 Switch to the `sdc` user usingthe command: `sudo su - sdc`.

Step 3 View the connector log by running command `sdc eventing logs --type connector`.

Note
If the registration has failed due to an invalid token, you see an error message in the log file similar to the example below:

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

Step 4 Remove the SEC.

Step 5 Add a new SEC in the UI and re-onboard.

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 left pane, click **Events & Logs** > **Events** > **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.

Event Logging Troubleshooting Log Files

The Secure Event Connector troubleshooting command collects logs, configurations, and limited system information, compressing them into a single archive to simplify the diagnosis of issues. If you already have a TAC case open, the compressed archive can also be sent directly to your TAC representative.

1. SSH to your host using the admin account, typically `cdo`.
2. Switch to the SDC user using the command `sudo su - sdc`
3. **If you do not have a TAC case open:** Run the command to gather and compress the troubleshooting bundle:

   ```
   sdc eventing troubleshoot
   ```

4. **If you already have a TAC case open:** Request an upload token from your TAC representative and use the command to gather, compress, and upload the troubleshooting bundle directly to your case:

   ```
   sdc eventing troubleshoot --case-number [your-tac-case-number] --token
   [the-token-tac-provided]
   ```

5. If you prefer to retrieve the troubleshooting bundle manually, use SCP or SFTP. Locate the absolute path to the bundle provided in the last log entry after running the troubleshoot command. Then, use the following SCP command to download the bundle to your local machine:

   ```
   scp -P [22 or whichever port you SSH on]
           cdo@your-vm-ip:/opt/cdo/.cdo/troubleshooting/cdo_[tenant-name-here]
           -troubleshooting-[timestamp-here].tar.gz ./sec-troubleshooting-bundle.tar.gz
   ```



Note Replace
`/opt/cdo/.cdo/troubleshooting/cdo_\[tenant-name-here\]-troubleshooting-\[timestamp-here\].tar.gz`
with the actual path displayed in the log output.

If you want to decompress the archive to review the logs and system configurations, use the command:
`tar xvf ./[sec-troubleshooting-bundle-filename].tar.gz`

SEC Status is Inactive in Security Cloud Control

Symptom: The Secure Event Connector status shows "Inactive" in the Security Cloud Control Secure Connectors page after onboarding for one of these reasons:

- Heartbeat failed
- Connector registration failed

Repair:

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

The SEC is online, but there are no events in Security Cloud Control Event Logging Page

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

Solution or workaround:

Procedure

Step 1 SSH to your host using the admin account, typically `cdo`.

Step 2 Switch to the SDC user with the command `sudo su - sdc`.

Step 3 Perform the following checks:

- Check SEC connector log using the command `sdc eventing logs --type connector -n 100` and ensure the SEC registration was successful.

  If not, see Secure Event Connector Registration failure.

- Check SEC events log using the command `sdc eventing logs --type events -n 200` and ensure that the events are being processed.

  If not, contact Security Cloud Control support.

- Check the SEC supervisor log with `sdc eventing logs --type supervisor -n 100` and ensure the output is as shown below and all processes in **RUNNING** state.

  If not, contact Security Cloud Control support.

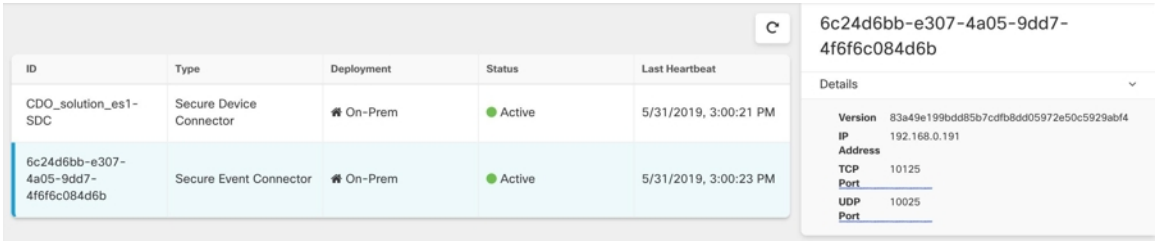
INFO success: estreamer-connector entered RUNNING state, process has stayed up for > than 1 seconds

INFO success: estreamer-plugin entered RUNNING state, process has stayed up for > than 1 seconds

INFO success: estreamer-rsyslog entered RUNNING state, process has stayed up for > than 1 seconds

- 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 Security Cloud Control support..

Remove an SEC from Your Host

The Secure Event Connector (SEC) delete command removes the SEC container along with its associated files from the Secure Device Connector (SDC) virtual machine. This command is typically used to address issues such as Secure Event Connector registration failures or onboarding failures.

To run the command:

Procedure

Step 1 SSH to your host using the admin account, typically `cdo`.

Step 2 Switch to the SDC user with `sudo su - sdc`.

Step 3 Run the command `sdc eventing delete`.

If applicable, you will be prompted to select the tenant you wish to delete. Follow the on-screen prompts to confirm your selection and fully remove the SEC data from the virtual machine.

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 SSH to your host using the admin account, typically `cdo`.

Step 2 Switch to the SDC user using the command `sudo su - sdc`

Step 3 Run the command `sdc eventing healthcheck` and, if applicable, select the tenant when prompted.

```
sdc@ci-sdc-4:~$ sdc eventing healthcheck
2025-05-06 16:36:20 [INFO] [ Manual Command ] even
2025-05-06 16:36:44 [INFO] Running SEC healthcheck



================================================

Running SEC health check for tenant CDO_blum-tenan
--

SEC cloud URL stage-api-sse.cisco.com is: Reachabl
SEC Connector status: Eventing subscription not en
okSEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
SEC netflow collector is: Running
Skipping SEC test event due to earlier failures
SEC healthcheck failed, please review any errors a
ok
================================================
```

Values of Health Check output:

- **SEC Cloud URL**: Displays the Security Cloud Control cloud URL and whether or not the SEC can reach Security Cloud Control.
- **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 Security Cloud Control.
- **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 Security Cloud Control

Troubleshooting login failures

Login Fails Because You are Inadvertently Logging in to the Wrong Security Cloud Control Region

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

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

Solution If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try the "forgot password" option and cannot recover a viable password, you may have tried to log in without creating a new Cisco Security Cloud Sign On account. You need to sign up for a new Cisco Security Cloud Sign On Account.

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

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control 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 created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Security Cloud Control APJ
  - **Solution** Security Cloud Control Australia
  - **Solution** Security Cloud Control EU
  - **Solution** Security Cloud Control India

- **Solution** Security Cloud Control US

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

Troubleshooting Access and Certificates

Troubleshoot User Access with Security Cloud Control

Consider the case of users being denied access to a resource that they should have access to. Here is an approach you can take to diagnose and remediate that problem.

Procedure

Step 1 Users inform your security team that their access to a resource is blocked. Determine how that resource is typically reached. What is it's IP address? Do you reach it on a specific port? What protocol is used to send information to the resource?

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select the ASA and run packet tracer. See ASA Packet Tracer for more instructions.

Step 4 Examine the packet trace table for rules that may have denied access to the resource.

Step 5 Edit the rule from Security Cloud Control to correct the behavior. Your ASA is now out of sync with Security Cloud Control.

Step 6 Deploy the changes to the ASA from the **Security Devices** page. Security Cloud Control traces packets through the configuration saved on the ASA not a configuration staged on Security Cloud Control. Be aware, you will also be deploying any other configuration changes staged on Security Cloud Control to your ASA.

Step 7 Re-run packet tracer to determine if the policy change provides the desired results. Confirm that your users now have access to the resource.

Step 8 Assuming your users now have access, clear the change request label in Security Cloud Control. This prevents unrelated activity from being associated with this fix.

Note
If the change you made doesn't fix the problem or creates some new problems and you want to return to your previous configuration, you can do restore the ASA Configuration.

See Restoring ASA Configurations.

Resolve New Fingerprint Detected State

Procedure

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

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Select the device in the **New Fingerprint Detected** state.

Step 6 Click **Review Fingerprint** in the New Fingerprint Detected pane.

Step 7 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 8 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 Security Cloud Control 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 left pane, click **Events & Logs** > **Events** > **Event Logging**.

Step 2 Click the **Historical** tab.

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

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

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

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

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

- **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.
- **FirewallPolicy** - The policy in which the rule that triggered the event resides.
- **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.

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

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

Troubleshooting SSL Decryption Issues

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

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

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

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

More Details

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

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

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

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

Solution If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try the "forgot password" option and cannot recover a viable password, you may have tried to log in without creating a new Cisco Security Cloud Sign On account. You need to sign up for a new Cisco Security Cloud Sign On Account.

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

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control 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 created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - **Solution** Security Cloud Control APJ
  - **Solution** Security Cloud Control Australia
  - **Solution** Security Cloud Control EU
  - **Solution** Security Cloud Control India
  - **Solution** Security Cloud Control US
- **Solution** Update your bookmark to point to https://sign-on.security.cisco.com.

Device connectivity states

You can view the connectivity states of the devices onboarded in your Security Cloud Control tenant. This topic helps you understand the various connectivity states. On the **Security Devices** 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 Security Cloud Control. 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, Security Cloud Control 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 Security Cloud Control.	NA

Device Connectivity State	Possible Reasons	Resolution
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 33
Invalid credentials	Username and password combination used by Security Cloud Control to connect to the device is incorrect.	Troubleshoot Invalid Credentials, on page 34
Onboarding	Device onboarding is initiated but is not complete.	Check you device's connectivity and ensure you complete the device registration.
Unknown	Device onboarding failed and Security Cloud Control cannot fetch the connectivity state of the device.	On the **Security Devices** page, select the device and choose **Check for Changes** from the right pane, to attempt fetching the latest configuration from the device.
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 34
Onboarding Error	Security Cloud Control may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error, on page 42

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 In the **Security Devices** 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, Security Cloud Control 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 Security Cloud Control.

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

d) In the Security Cloud Control area, expand **Get Started**.
e) In the **Registration Key** field, paste the registration key that you generated in Security Cloud Control.
f) Click **Register** and then **Accept** the Cisco Disclosure. Firewall Device Manager sends the registration request to Security Cloud Control.
g) Refresh the **Security Devices** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
h) Click **Read Configuration** for Security Cloud Control to read the configuration from the device.

Step 4 If the unregistered device was onboarded using the serial number, Security Cloud Control 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 Security Cloud Control.
b) Under **System Settings**, click **Cloud Services**.
c) Select the **Auto-enroll with Tenancy from Security Cloud Control** option and click **Register**.
d) Refresh the **Security Devices** page in Security Cloud Control until you see the device's connectivity state changes to "Read Error".
e) Click **Read Configuration** for Security Cloud Control 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 Security Cloud Control portal by signing out from Security Cloud Control 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 left pane, click the **Inventory** page.

Step 3 In the left pane, click **Security Devices**.

Step 4 Click the **Devices** tab.

Step 5 Click the appropriate device type tab and select the device with the **Insufficient License** state.

Step 6 In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.

Step 7 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 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab and select the device with the **Invalid Credentials** state.

Step 5 In the **Device Details** pane, click **Reconnect** appearing in **Invalid Credentials**. Security Cloud Control attempts to reconnect with your device.

Step 6 When prompted enter the new username and password for the device.

Step 7 Click **Continue**.

Step 8 After the device is online and ready to use, click **Close**.

Step 9 It is likely that because Security Cloud Control attempted to use the wrong credentials to connect to the device, the username and password combination Security Cloud Control 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 Security Cloud Control and the device.

Troubleshoot New Certificate Issues

Security Cloud Control's Use of Certificates

Security Cloud Control checks the validity of certificates when connecting to devices. Specifically, Security Cloud Control 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 Security Cloud Control uses certificates differently than browsers:

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

Identifying Certificate Issues

There are several reasons that Security Cloud Control may not be able to onboard a device. When the UI shows a message that "Security Cloud Control 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 Security Cloud Control rejects a given certificate, you can use the openssl command-line tool on the SDC host or another host that can reach the relevant device. Use the following command to create a file showing the certificates presented by the device:

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

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

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

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
```

```
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

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

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

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

0 X509_V_OK The operation was successful.

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

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

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

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

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

7 X509_V_ERR_CERT_SIGNATURE_FAILURE The signature of the certificate is invalid.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE The signature of the certificate is invalid.

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

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

11 X509_V_ERR_CRL_NOT_YET_VALID The CRL is not yet valid.

12 X509_V_ERR_CRL_HAS_EXPIRED The CRL has expired.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD The certificate notBefore field contains an invalid time.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD The certificate notAfter field contains an invalid time.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD The CRL lastUpdate field contains an invalid time.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD The CRL nextUpdate field contains an invalid time.

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

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

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

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

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

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

23 X509_V_ERR_CERT_REVOKED The certificate has been revoked.

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

25 X509_V_ERR_PATH_LENGTH_EXCEEDED The basicConstraints pathlength parameter has been exceeded.

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

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

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

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

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

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

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

50 X509_V_ERR_APPLICATION_VERIFICATION An application specific error. Unused.

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, Security Cloud Control 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 Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Use the following procedure to resolve a new certificate:

1. Navigate to the **Inventory** page.
2. In the left pane, click **Security Devices**.
3. Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.
4. In the action pane, click **Review Certificate**. Security Cloud Control allows you to download the certificate for review and accept the new certificate.
5. In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

   Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

Certificate Error Codes

Verify return code: 0 (ok) but Security Cloud Control returns certificate error

Once Security Cloud Control 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, Security Cloud Control 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 Security Cloud Control 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, Security Cloud Control 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 Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Use the following procedure to resolve a new certificate:

Procedure

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

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.

Step 6 In the action pane, click **Review Certificate**. Security Cloud Control allows you to download the certificate for review and accept the new certificate.

Step 7 In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

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 In the left pane, click **Security Devices**.

Step 3 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 4 Remove the device instance from Security Cloud Control and try onboarding the device again.

Resolve the conflict detected status

Security Cloud Control 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 Security Cloud Control, the device's configuration status will show **Conflict Detected**.

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

Procedure

Step 1 Choose **Security Devices**.

Note
For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **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 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 Security Cloud Control.
- 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** Security Cloud Control with the device's running configuration.

  Note
  As Security Cloud Control 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 Security Cloud Control.

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 Choose **Inventory**.

Note
For an On-Premises 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 Choose **Security Devices**.

Note
For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device reported as Not Synced.

Step 6 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 Security Cloud Control 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 Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control 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 left pane, click **Security Devices**.

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 Security Cloud Control 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 Security Cloud Control 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 Security Cloud Control.

- For the RMA case, you need to perform the following steps in Security Cloud Control:

  1. If the device was successfully onboarded, you need to save the device configuration as a template.

     Remove the device instance from Security Cloud Control.

  2. Power on the new replacement device that you have received from the RMA team and onboard it to Security Cloud Control.

     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 Security Cloud Control and the device.

- 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 Security Cloud Control.