

Secure Event Connectors

This chapter provides information about secure event connectors.

- Secure event connectors, on page 1
- Secure event connector installation, on page 2
- Secure event connector removal, on page 22
- Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS), on page 23

Secure event connectors

A Secure Event Connector (SEC) is a component of the Security Analytics and Logging SaaS solution that

- receives events from ASA , and FDM-managed devices
- forwards events to the Cisco cloud for centralized analysis, and
- enables display of events on the **Event Logging** page in Security Cloud Control.

SEC deployment options

The SEC is installed on a Secure Device Connector deployed in your network, on its own Security Cloud Control Connector virtual machine deployed in your network, or on an AWS Virtual Private Cloud (VPC).

Secure Event Connector ID location:

1. From the Security Cloud Control menu on the left, choose **Tools & Services** > **Secure ConnectorsAdministration** > **Secure Connectors**.
2. Click the SEC you wish to identify.
3. The SEC ID is the ID listed above the Tenant ID in the Details pane.

Note You may need the ID of the SEC when working with Cisco Technical Assistance Center (TAC) or other Security Cloud Control Support.

Secure event connector installation

A Secure Event Connector installation is a deployment process that enables installation of SECs on a tenant with or without an SDC configuration.

Installation options

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own Security Cloud Control Connector virtual machine that you maintain in your network.

Install a secure event connector on an SDC virtual machine

The purpose of this task is to install a Secure Event Connector on an existing SDC virtual machine to enable centralized event logging and analysis.

The Secure Event Connector (SEC) receives events from ASA and FDM-managed devices and forwards them to the Cisco cloud. Security Cloud Control displays the events on the **Event Logging** page enabling you to analyze the security events from all devices in one place.

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own Security Cloud Control Connector virtual machine that you maintain in your network.

This article describes installing an SEC on the same virtual machine as an SDC. If you want to install more SECs see Installing an SEC using a Security Cloud Control image, on page 4 or SEC installation using VM images, on page 10.

Before you begin

- Purchase the Cisco Security and Analytics Logging license. If you want to try Cisco Security and Analytics Logging out first, log in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** > **Event Logging** and click **Request Trial**.
- Make sure the SDC is communicating with Security Cloud Control:
  1. In the left pane, click **Tools & Services** > **Secure ConnectorsAdministration** > **Secure Connectors**.
  2. Make sure that the SDC's last heartbeat was less than 10 minutes prior to the installation of the SEC and that the SDC's status is active.
- System Requirements - Assign additional CPUs and memory to the virtual machine running the SDC:
  - CPU: Assign an **additional** 4 CPUs to accommodate the SEC to make a total of 6 CPU.
  - Memory: Assign an **additional** 8 GB of memory for the SEC to make a total of 10 GB of memory.

    After you have updated the CPU and memory on the VM to accommodate the SEC, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.

Follow these steps to install a Secure Event Connector on an SDC virtual machine:

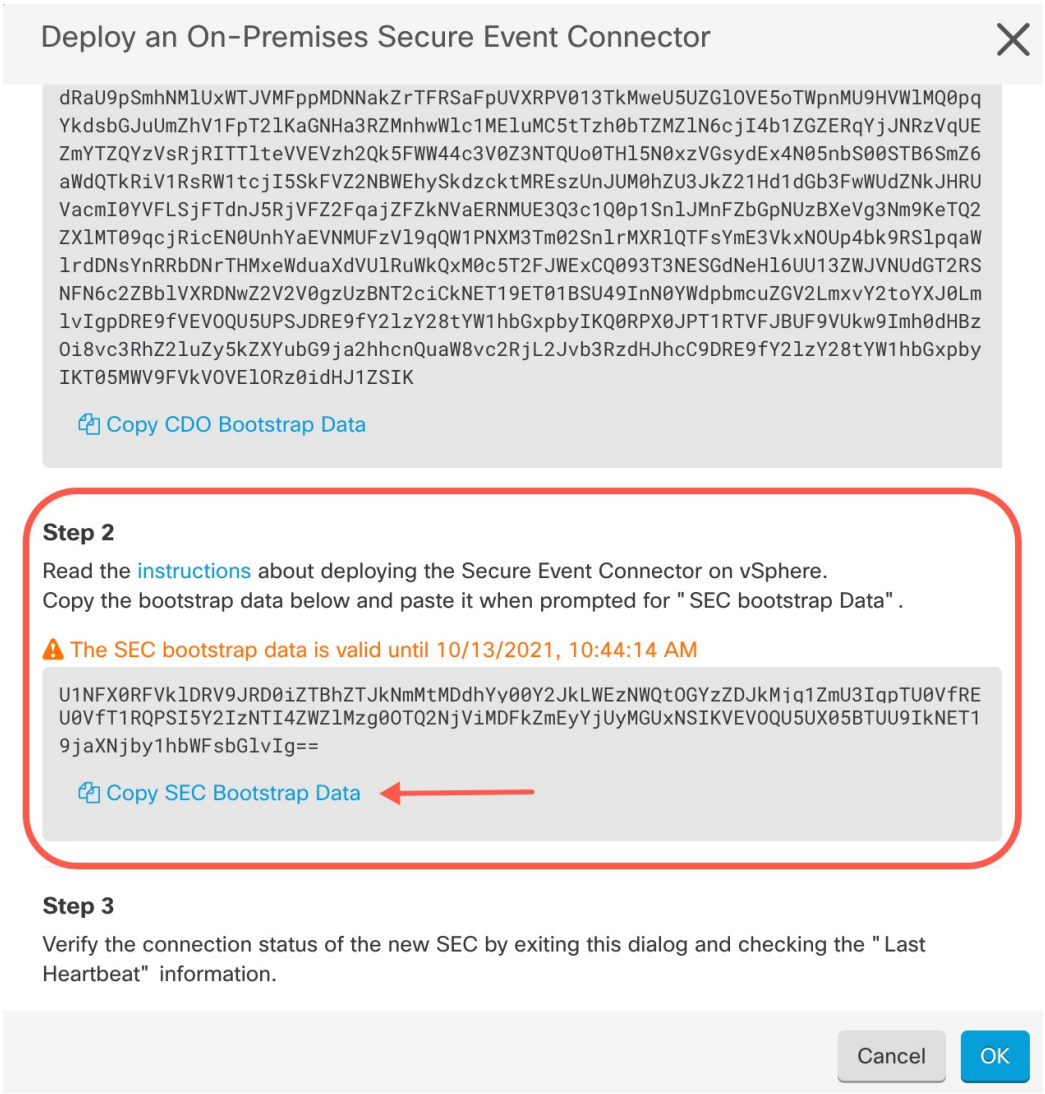
Procedure

Step 1 Log in to Security Cloud Control.

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

Step 3 Click the + icon and then click **Secure Event Connector**.

Step 4 Skip Step 1 of the wizard and go to Step 2. In step 2 of the wizard, click the link to **Copy SEC Bootstrap Data**.



Step 5 Open a terminal window and log into the SDC as the "cdo" user.

Step 6 Once logged in, switch to the "SDC" user. When prompted for a password, enter the password for the "cdo" user.

Example:

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

Step 7 At the prompt, run the **SEC.sh setup** script:

Example:

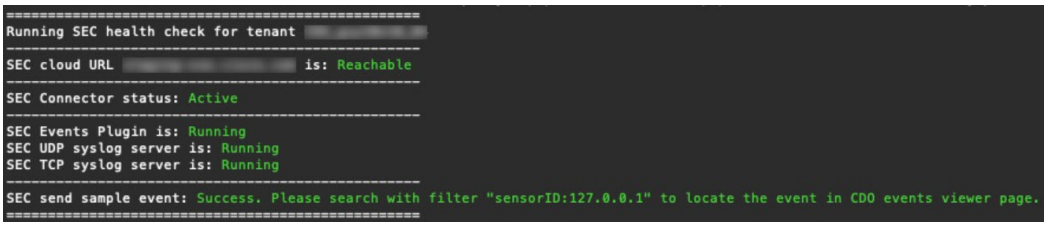
```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 8 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Example:

```
Please copy the bootstrap data from Setup Secure Event Connector page of Security Cloud
Control: KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the SEC.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "SEC-health-check."



Step 9 Determine if the VM on which the SDC and SEC are running needs additional configuration:

- If you installed your SDC on your own virtual machine, continue with Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created, on page 16.
- If you installed your SDC using a Security Cloud Control image, continue to "What to do Next."

The Secure Event Connector is now installed on your SDC virtual machine and is ready to receive events from ASA devices and forward them to the Cisco cloud for analysis in the Event Logging page.

Installing an SEC using a Security Cloud Control image

Installing an SEC using a Security Cloud Control image is a deployment process that

- enables the Secure Event Connector (SEC) to forward events from ASA and FTD devices to the Cisco cloud for viewing in the **Event Logging** page
- allows installation of multiple SECs on a tenant to distribute event forwarding workload across different locations, and
- requires a two-part process involving Security Cloud Control Connector installation and SEC configuration.

Installation process

Installing an SEC is a two-part process:

1. Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image, on page 5 You need one Security Cloud Control Connector for every SEC you install. The Security Cloud Control Connector is different than a Secure Device Connector (SDC).
2. Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine, on page 18.



Note If you want to create a Security Cloud Control Connector by creating your own VM, see Install Multiple SECs for Your Tenant Using a VM Image you Create.

What to do next:

Continue with Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image, on page 5

Install a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image

Install a Security Cloud Control Connector on a virtual machine to provide the platform for deploying a Secure Event Connector that will handle security event logging and analytics.

This task is performed when you need to set up a Security Cloud Control Connector as the foundation for a Secure Event Connector deployment in your network infrastructure.

Before you begin

- Purchase the Cisco Security and Analytics Logging license.

  If you would rather, you can request a trial version of Security Analytics and Logging by logging in to Security Cloud Control, and on the main navigation bar, choose **Events & Logs** > **Events** > **Event Logging** and click **Request Trial**.

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the Security Cloud Control Connector and the Internet. If using a proxy server, disable inspection for traffic between the Security Cloud Control Connector and Security Cloud Control.
- **The** Security Cloud Control **Connector installed in this process must have full outbound access to the Internet on TCP port 443.**
- Security Cloud Control supports installing its Security Cloud Control Connector VM OVF image using the vSphere web client or the ESXi web client.
- Security Cloud Control does not support installing the Security Cloud Control Connector VM OVF image using the VM vSphere desktop client.
- ESXi 5.1 hypervisor.
- System requirements for a VM intended to host only a Security Cloud Control Connector and an SEC:
  - VMware ESXi host needs 4 vCPU.
  - VMware ESXi host needs a minimum of 8 GB of memory.
  - VMware ESXi requires 64GB disk space to support the virtual machine depending on your provisioning choice.

- Gather this information before you begin the installation:
  - Static IP address you want to use for your Security Cloud Control Connector VM.
  - Passwords for the **root** and Security Cloud Control users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the SDC address is on.
  - The FQDN or IP address of your time server.
- The Security Cloud Control Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

Follow these steps to install a Security Cloud Control Connector using a VM image:

Procedure

Step 1 Log on to the Security Cloud Control tenant you are creating the Security Cloud Control Connector for.

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

Step 3 Click the + icon and then click **Secure Event Connector**.

Step 4 In Step 1, click **Download the Security Cloud Control Connector VM image**. This is a special image that you install the SEC on. Always download the Security Cloud Control Connector VM to ensure that you are using the latest image.



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

- Security Cloud Control-SDC-VM-ddd50fa.OVF
- Security Cloud Control-SDC-VM-ddd50fa.mf
- Security Cloud Control-SDC-VM-ddd50fa-disk1.vmdk

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

Note
Do not use the VM vSphere desktop client.

Step 7 Deploy the on-premises Security Cloud Control Connector virtual machine from the OVF template by following the prompts. (You will need the .OVF, .mf, and .vdk files to deploy the template.)

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

Step 9 Open the console for your new Security Cloud Control Connector VM.

Step 10 Login as the Security Cloud Control user. The default password is **adm123**.

Step 11 At the prompt type **sudo SDC-onboard setup**

Example:

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

Step 12 When prompted, enter the default password for the Security Cloud Control user: **adm123**.

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

Step 14 Follow the prompts to create a new password for the Security Cloud Control user.

Step 15 Follow the prompts to enter your Security Cloud Control domain information.

Step 16 Enter the static IP address you want to use for the Security Cloud Control Connector VM.

Step 17 Enter the gateway IP address for the network on which the Security Cloud Control Connector VM is installed.

Step 18 Enter the NTP server address or FQDN for the Security Cloud Control Connector.

Step 19 When prompted, enter the information for the Docker bridge or leave it blank if it is not applicable and press <Enter>.

Step 20 Confirm your entries.

Step 21 When prompted "Would you like to setup the SDC now?" enter **n**.

Step 22 Create an SSH connection to the Security Cloud Control Connector by logging in as the Security Cloud Control user.

Step 23 At the prompt type **sudo SDC-onboard bootstrap**

Example:

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

Step 24 When prompted, enter the Security Cloud Control user's password.

Step 25 When prompted, return to Security Cloud Control and copy the Security Cloud Control bootstrap data, then paste it into your SSH session. To copy the Security Cloud Control bootstrap data:

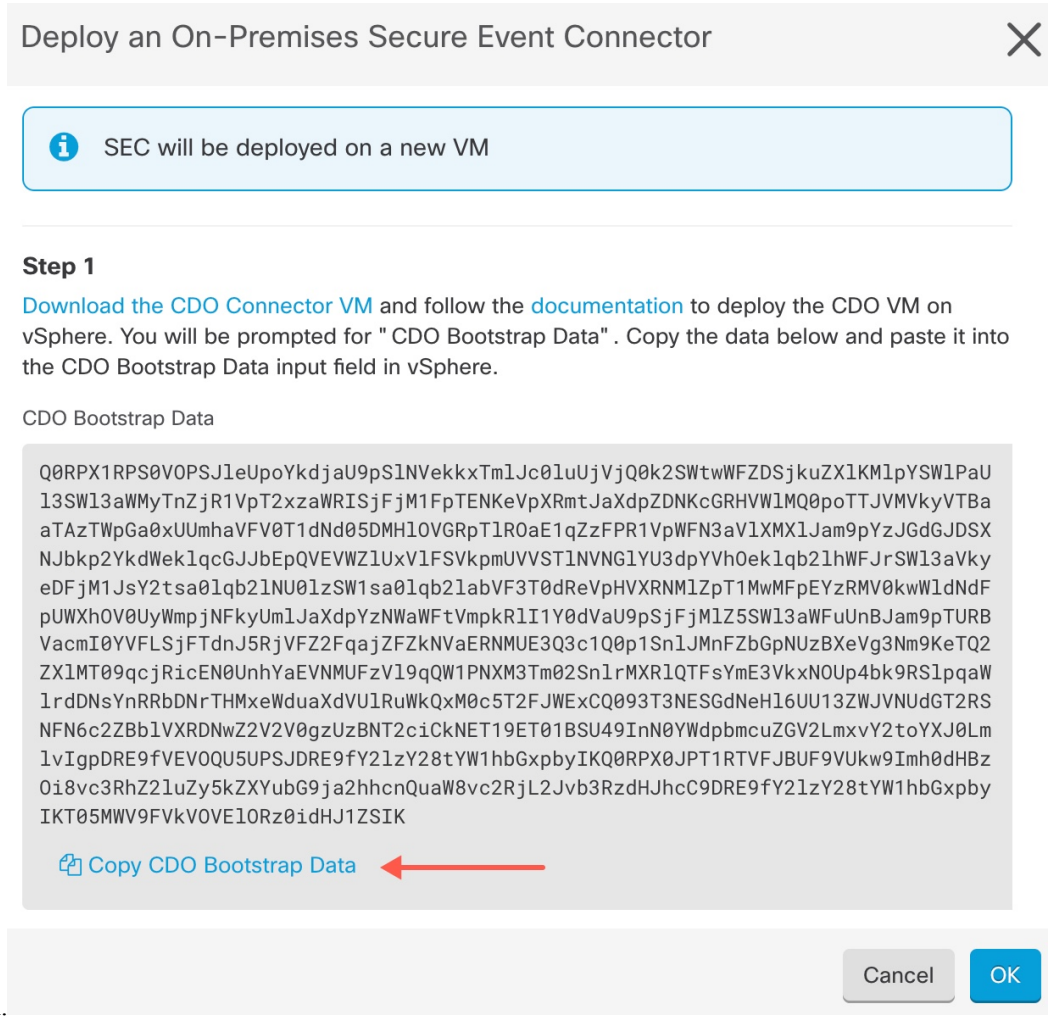
a. Log into Security Cloud Control.

b. In the left pane, click **Tools & Services** > **Secure ConnectorsAdministration** > **Secure Connectors**.

c. Select the Secure Event Connector which you started to onboard. The status should show, "Onboarding."

d. In the **Actions** pane, click **Deploy an On-Premises Secure Event Connector**.

e. Copy the Security Cloud Control Bootstrap Data in step 1 of the dialog box.



Step 26 When prompted, **Would you like to update these settings?** enter **n**.

Step 27 Return to the **Deploy an On-Premises Secure Event Connector** dialog in Security Cloud Control and click **OK**. In the **Secure Connectors** page, you will see your Secure Event Connector is in the yellow Onboarding state.

Continue to Install the Secure Event Connector on the Security Cloud Control Connector VM, on page 8.

Your Security Cloud Control Connector VM is successfully installed and configured, with the Secure Event Connector in an onboarding state ready for the next installation phase.

Install the Secure Event Connector on the Security Cloud Control Connector VM

This task enables secure event logging by installing and configuring the Secure Event Connector on your Security Cloud Control Connector VM to establish communication between on-premises devices and the cloud-based logging service.

The Secure Event Connector enables secure logging analytics for your security devices by creating a secure tunnel between your on-premises environment and the cloud logging service. This connector must be properly installed and configured to ensure events are successfully transmitted and logged.

Before you begin

You should have installed Security Cloud Control Connector VM as described inInstall a Security Cloud Control Connector, to Support a Secure Event Connector, Using a Security Cloud Control VM Image, on page 5 .

Follow these steps to install the Secure Event Connector on the Security Cloud Control Connector VM:

Procedure

Step 1 Log in to Security Cloud Control.

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

Step 3 Select the Security Cloud Control Connector that you onboarded above. In the Secure Connectors table, it will be called a Secure Event Connector and it should still be in the "Onboading" status.

Step 4 Click **Deploy an On-Premises Secure Event Connector** in the Actions pane on the right.

Step 5 In **step 2** of the wizard, click the link to **Copy SEC bootstrap data**.

Step 6 Create an SSH connection to the Security Cloud Control Connector and log in as the **CDO** user.

Step 7 Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "Security Cloud Control" user. Here is an example of those commands:

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

Step 8 At the prompt, run the SEC.sh setup script:

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

Step 9 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the SEC.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "SEC-health-check."



If you receive the success message return to Security Cloud Control and click **Done on the Deploy an ON-Premise Secure Event Connector** dialog box.

Return to Implement secure logging analytics (SaaS) for ASA devices .

The Secure Event Connector is successfully installed and configured on the Security Cloud Control Connector VM. The connector establishes a secure communication channel for event logging, and a health check event appears in the Event Log confirming proper operation.

Deploy secure event connector on ubuntu virtual machine

Deploy the Secure Event Connector on your Ubuntu VM to enable event collection and management through CDO.

The Secure Event Connector allows you to collect and forward security events from your network devices to CDO for centralized monitoring and analysis. This deployment process requires bootstrap data from CDO to establish the secure connection.

Before you begin

Follow these steps to deploy Secure Event Connector on Ubuntu Virtual Machine:

Procedure

Step 1 Log on to Security Cloud Control.

Step 2 From the left pane, **Tools & Services** > **Secure ConnectorsAdministration** > **Secure Connectors**.

Step 3 Click the  icon and then click **Secure Event Connector**.

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

Step 5 Execute the following commands:

```
[sdc@vm]:~$sudo su sdc
```

```
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

When prompted, enter the SEC bootstrap data that you have copied.

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

It may take a few minutes for the Secure Event Connector to become "Active" in Security Cloud Control.

The Secure Event Connector is successfully deployed and becomes "Active" in CDO, enabling event collection and forwarding from your network devices.

SEC installation using VM images

A SEC installation using VM images is a deployment method that

- forwards events from ASA and FTD to the Cisco cloud so that you can view them in the **Event Logging** page in Security Cloud Control

- allows installation of multiple Secure Event Connectors on your tenant to direct events from your ASAs and FDM-managed devices to any of the SECs you install, and
- enables distribution of event forwarding work across different regions by having SECs installed in different locations.

Installation process requirements

Installing multiple SECs using your own VM image requires completion of these steps:

1. Install a Security Cloud Control Connector to Support an SEC Using Your VM Image , on page 11
2. Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created, on page 16
3. Install the Secure Event Connector



Note Using a Security Cloud Control VM image for the Security Cloud Control Connector is the easiest, most accurate, and preferred method of installing a Security Cloud Control connector. If you want to use that method, see Installing an SEC using a Security Cloud Control image, on page 4.

Continue to Install a Security Cloud Control Connector to Support an SEC Using Your VM Image , on page 11 to begin the installation process.

Install a Security Cloud Control Connector to Support an SEC Using Your VM Image

To install and configure a Secure Event Connector (SEC) on a virtual machine so it can securely transmit event data to Cisco Security Analytics and Logging (SaaS). This ensures proper integration and secure communication between your organization's environment and Cisco's security analytics platform.

The Security Cloud Control Connector VM is a virtual machine on which you install an SEC. The purpose of the Security Cloud Control Connector is solely to support an SEC for Cisco Security Analytics and Logging (SaaS) customers.

This is the first of three steps you need to complete in order install and configure your Secure Event Connector (SEC). After this procedure, you need to complete the following procedures:

- Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created, on page 16
- Install the Secure Event Connector

Before you begin

- Purchase a Security and Analytics Logging (SaaS) subscription plan. For more information about the subscription plans, refer to the Security Cloud Control Firewall Management Ordering Guide .

  If you would rather, you can request a trial version of Security Analytics and Logging by logging in to Security Cloud Control , and on the main navigation bar, choose **Events & Logs** > **Events** > **Event Logging** and click **Request Trial** .
- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the Security Cloud Control Connector and the Internet.

- **The Security Cloud Control Connector must have full outbound access to the Internet on TCP port 443.**
- VMware ESXi host installed with vCenter web client or ESXi web client.

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

- ESXi 5.1 hypervisor.
- Ubuntu 22.04 and Ubuntu 24.04.
- System requirements for a VM to host only a Security Cloud Control Connector and an SEC:
  - CPU: Assign 4 CPUs to accommodate the SEC.
  - Memory: Assign 8 GB of memory for the SEC.
  - Disk Space: 64 GB
- Users performing this procedure should be comfortable working in a Linux environment and using the **vi** visual editor for editing files.
- Gather this information before you begin the installation:
  - Static IP address you want to use for your Security Cloud Control Connector.
  - Passwords for the **root** and **Security Cloud Control** users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the Security Cloud Control Connector address is on.
  - The FQDN or IP address of your time server.
- The Security Cloud Control Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.
- **Before you get started** : Do not copy and paste the commands in this procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

Procedure

Step 1 Log on to Security Cloud Control .

Step 2 From the left pane, **Tools & Services** > **Secure ConnectorsAdministration** > **Secure Connectors** .

Step 3 Click the + icon and then click **Secure Event Connector** .

Step 4 Using the link provided, copy the SEC Bootstrap Data in step 2 of the "Deploy an On-Premises Secure Event Connector" window.

Step 5 Once installed, configure basic networking such as specifying the IP address for the Security Cloud Control Connector, the subnet mask, and gateway.

Step 6 Configure a DNS (Domain Name Server) server.

Step 7 Configure a NTP (Network Time Protocol) server.

Step 8 Install an SSH server for easy interaction with Security Cloud Control Connector's CLI.

Step 9 Install the **AWS CLI package** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)

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

Step 10 Install the **Docker CE packages** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)

Note
Use the "Install using the repository" method.

Step 11 Start the Docker service and enable it to start on boot:

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

Step 12 Create two users: **Security Cloud Control** and **sdc.** The Security Cloud Control user will be the one you log-into to run administrative functions (so you don't need to use the root user directly), and the sdc user will be the user to run the Security Cloud Control Connector docker container.

```
                        [root@sdc-vm ~]#
                        useradd
                        Security Cloud Control
 [root@sdc-vm ~]#
                        useradd sdc -d /usr/local/
                        Security Cloud Control
```

Step 13 Configure the sdc user to use crontab:

```
                        [root@sdc-vm ~]#
                        touch /etc/cron.allow
[root@sdc-vm ~]#
                        echo "sdc" >> /etc/cron.allow
```

Step 14 Set a password for the Security Cloud Control user.

```
                        [root@sdc-vm ~]#
                        passwd
                        Security Cloud Control
Changing password for user
                        Security Cloud Control
                        .
New password:
                        <type password>
```

```
Retype new password:
                        <type password>
passwd: all authentication tokens updated successfully.
```

Step 15 Add the Security Cloud Control user to the "wheel" group to give it administrative (sudo) privileges.

```
                        [root@sdc-vm ~]#
                        usermod -aG wheel
                        Security Cloud Control
 [root@sdc-vm ~]#
```

Step 16 When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

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

Step 17 If the `/etc/docker/daemon.json` file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

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

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

Step 18 If you are currently using a vSphere console session, switch over to SSH and log in as the **Security Cloud Control** user. Once logged in, change to the **sdc** user. When prompted for a password, enter the password for the **Security Cloud Control** user.

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

```
[sdc@sdc-vm ~]$
```

Step 19 Change directories to **/usr/local/** Security Cloud Control **.**

Step 20 Create a new file called **bootstrapdata** and paste the bootstrap data from Step 1 of the deployment wizrd into this file. **Save** the file. You can use **vi** or **nano** to create the file.

Step 21 The bootstrap data comes encoded in base64. Decode it and export it to a file called **extractedbootstrapdata**

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

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

```
                         [sdc@sdc-vm ~]$
                         cat /usr/local/
                         Security Cloud Control
                         /extractedbootstrapdata
                         Security Cloud Control
                         _TOKEN="<token string>"
                         Security Cloud Control
                         _DOMAIN="www.defenseorchestrator.com"
                         Security Cloud Control
                         _TENANT="<tenant-name>"
<
                         Security Cloud Control
                         _URL>/sdc/bootstrap/
                         Security Cloud Control

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

Step 22 Run the following command to export the sections of the decoded bootstrap data to environment variables.

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

Step 23 Download the bootstrap bundle from Security Cloud Control .

```
                          [sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $
                         Security Cloud Control
                         _TOKEN" "$
                         Security Cloud Control
                         _BOOTSTRAP_URL" -o $
                         Security Cloud Control
                         _TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$
                         ls -l /usr/local/
                         Security Cloud Control
                         /*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/
                         Security Cloud Control
                         /
```

```
                                    Security Cloud Control
                                    _<tenant_name>
```

Step 24 Extract the Security Cloud Control Connector tarball, and run the bootstrap_sec_only.sh file to install the Security Cloud Control Connector package.

```
                                     [sdc@sdc-vm ~]$
                                    tar xzvf /usr/local/
                                    Security Cloud Control
                                    /tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$
                                    /usr/local/
                                    Security Cloud Control
                                    /bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/
                                    Security Cloud Control
                                    /toolkit/es_toolkit.sh upgradeEventing 2>&1 >> /usr/local/
                                    Security Cloud Control
                                    /toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/
                                    Security Cloud Control
                                    /toolkit/es_toolkit.sh es_maintenance 2>&1 >> /usr/local/
                                    Security Cloud Control
                                    /toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

Continue to Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created, on page 16 .

Your Secure Event Connector (SEC) is installed on your VM image, configured to securely forward events to Cisco Security Analytics and Logging (SaaS), and ready for ongoing maintenance and updates.

Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created

This configuration ensures that events can reach the SEC when you have installed your Security Cloud Control Connector on your own CentOS 7 virtual machine.

This is the second of three steps you need to complete in order to install and configure your SEC. If you have not already, complete Install a Security Cloud Control Connector to Support an SEC Using Your VM Image , on page 11 before making these configuration changes.

After you complete one of the additional configuration changes described here, complete Install the Secure Event Connector

Before you begin

You must have installed your Security Cloud Control Connector on your own CentOS 7 virtual machine.

Follow these steps to configure additional settings for your SDC and Security Cloud Control Connector:

Procedure

Step 1 Choose one of the following configuration procedures:

- Disable the firewalld service on the CentOS 7 VM (matches the configuration of the Cisco-provided SDC VM)
- Allow the firewalld service to run and add firewall rules to allow event traffic to reach the SEC (more granular approach)

Step 2 If you chose to disable the firewalld service, log into the CLI of the SDC VM as the "Security Cloud Control" user.

Step 3 Stop the firewalld service and ensure that it will remain disabled upon subsequent reboots of the VM.

If you are prompted, enter the password for the **Security Cloud Control** user.

Example:

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl stop firewalld
Security Cloud Control@SDC-VM ~]$ sudo systemctl disable firewalld
```

Step 4 Restart the Docker service to re-insert Docker-specific entries into the local firewall.

Example:

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart docker
```

Step 5 If you chose to allow the firewalld service to run, log into the CLI of the SDC VM as the "Security Cloud Control" user.

Step 6 Add local firewall rules to allow incoming traffic to the SEC from the TCP, UDP, or NSEL ports you configured.

See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging for the ports used by your SEC. If prompted, enter the password for the **Security Cloud Control** user. You may need to specify different port values.

Example:

```
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10125/tcp
Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10025/udp
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10425/udp
```

Step 7 Restart the firewalld service to make the new local firewall rules both active and persistent.

Example:

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart firewalld
```

You have successfully configured the firewall settings on your CentOS 7 virtual machine to allow events to reach the SEC.

What to do next

Continue to Install the Secure Event Connector.

Install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine

This procedure completes the installation and configuration of your Secure Event Connector (SEC) on your virtual machine, enabling secure event logging and analytics capabilities.

This is the final step in a three-part process to deploy a Secure Event Connector. The SEC enables secure event logging and analytics for your devices managed through Security Cloud Control.

Before you begin

This is the third of three steps you need to complete in order to install and configure your Secure Event Connector (SEC). If you have not already, complete the following tasks before continuing with this procedure:

- Install a Security Cloud Control Connector to Support an SEC Using Your VM Image , on page 11.
- Configure additional settings for SDCs and Security Cloud Control Connectors installed on a VM you created, on page 16.

Follow these steps to install the Secure Event Connector on your Security Cloud Control Connector Virtual Machine:

Procedure

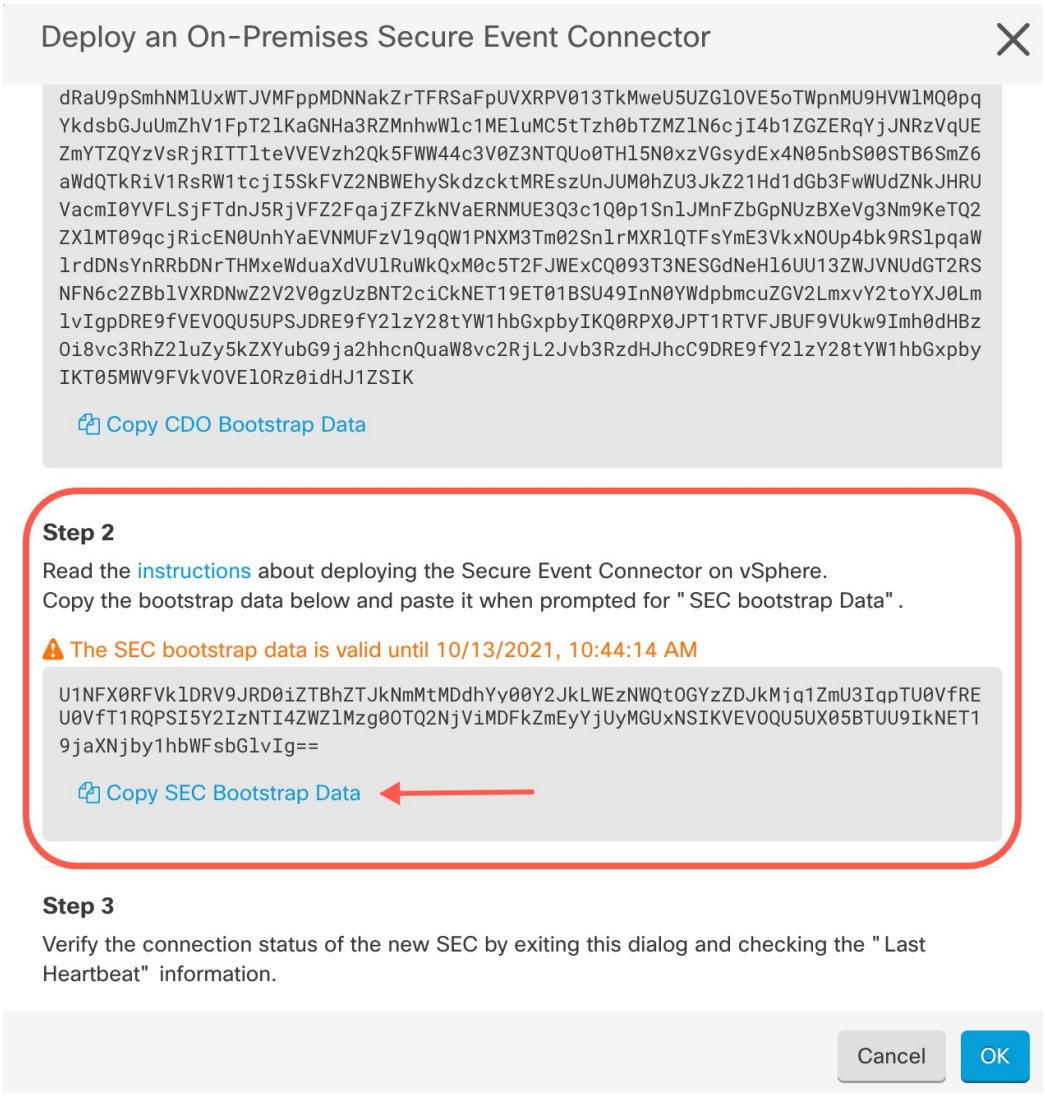
Step 1 Log in to Security Cloud Control.

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

Step 3 Select the Security Cloud Control Connector that you installed using the procedure in the prerequisites above. In the Secure Connectors table, it will be displayed as Secure Event Connector.

Step 4 Click **Deploy an On-Premises Secure Event Connector** in the **Actions** pane on the right.

Step 5 In **step 2** of the wizard, click the link to **Copy SEC Bootstrap Data**.



Step 6 Connect to the Secure Connector using SSH and log in as the Security Cloud Control user.

Step 7 Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "Security Cloud Control" user. Here is an example of those commands:

Example:

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

Step 8 At the prompt, run the SEC.sh setup script:

Example:

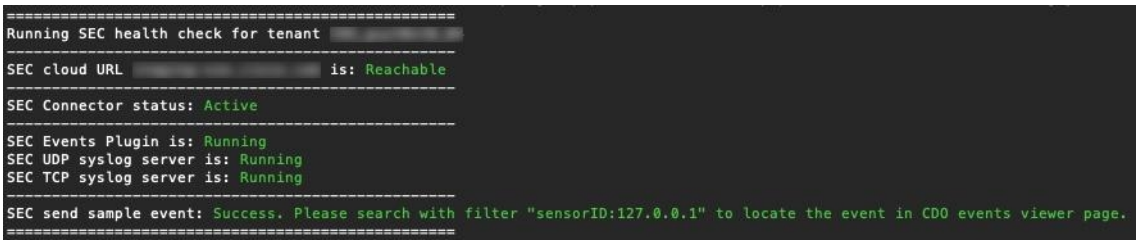
```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 9 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Example:

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the SEC.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "SEC-health-check."



If you receive the success message, click **Done** in the **Deploy an ON-Premise Secure Event Connector** dialog box.You have finished installing an SEC on a your VM image.

Return to this procedure to continue your implementation of SAL SaaS: Implement secure logging analytics (SaaS) for ASA devices.

The Secure Event Connector is successfully installed and configured on your virtual machine. The SEC performs health checks and sends a sample event to verify proper operation.

Install a secure event connector on an AWS VPC using a terraform module

This task enables you to deploy a secure event connector on your AWS VPC infrastructure using Terraform automation, allowing for secure log collection and transmission to Security Cloud Control.

Use this procedure when you need to establish a secure event connector in an AWS VPC environment for centralized logging and analytics. The Terraform module automates the deployment process and ensures proper security configurations.

Before you begin

- To perform this task, you must enable SAL on your Security Cloud Control tenant. This section presumes that you have a SAL license. If you do not have one, purchase the Cisco Security and Analytics Logging, Logging and Troubleshooting license.
- Ensure you have a new SEC installed. To create a new SEC, see Install a secure event connector on an SDC virtual machine, on page 2.
- When installing the SEC, make sure you take a note of the Security Cloud Control bootstrap data and SEC bootstrap data.

Follow these steps to install a secure event connector on an AWS VPC using a Terraform module:

Procedure

Step 1 Go to Secure Event Connector Terraform Module on the Terraform Registry and follow the instructions to add the SEC Terraform module to your Terraform code and apply.

Step 2 Ensure that you print the **instance_id** and **sec_fqdn** outputs, because you will need them later in the procedure.

Note
To troubleshoot your SEC, you must connect to your SEC instance using the AWS Systems Manager Session Manager (SSM). See the AWS Systems Manager Session Manager documentation to know more about connecting to an instance using SSM.

Ports to connect to the SDC instance using SSH are not exposed for secuirty reasons.

Step 3 To enable sending of logs from your ASA to the SEC, obtain the certificate chain of the SEC you created and remove the leaf certificate by running this command with the output from Step 3:

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 <
 /dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++};
out="/tmp/cert_chain.pem"; if(a > 1) print >>out}'
```

Step 4 Copy the contents of **/tmp/cert_chain.pem** to your clipboard.

Step 5 Take a note of the IP address of the SEC using this command:

```
nslookup <FQDN>
```

Step 6 Log in to Security Cloud Control and start adding a new trustpoint object.

See Adding a Trusted CA Certificate Object for more information. Ensure you uncheck the **Enable CA flag in basic constraints extension** checkbox in **Other Options** before clicking **Add**.

Step 7 Click **Add**, copy the CLI commands generated by Security Cloud Control in the **Install Certificate** page, and click **Cancel**.

Step 8 Below **enrollment terminal**, add **no CA-check** in a text clipboard.

Step 9 SSH into your ASA device or use the ASA CLI option in Security Cloud Control and execute these commands:

```
DataCenterFW-1> en
Password: *****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

What to do next: You can check if your SEC is receiving packets using AWS SSM:

You should now see logs similar to this:

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

The secure event connector is successfully deployed on your AWS VPC and configured to receive logs from your ASA device. The SEC will begin processing and forwarding security events to Security Cloud Control for analysis and monitoring.

Secure event connector removal

Secure Event Connector removal is a process that

- deletes the Secure Event Connector from the Secure Device Connector
- prevents the use of Secure Logging Analytics (SaaS), and
- is not reversible once completed.

Removal process

Warning This procedure deletes the Secure Event Connector from the Secure Device Connector. Doing so will prevent you from using Secure Logging Analytics (SaaS). It is not reversible. If you have any questions or concerns, contact Security Cloud Control support before taking this action.

Removing the Secure Event Connector from your Secure Device Connector is a two-step process:

1. Remove SEC from Security Cloud Control.
2. Remove SEC files from the SDC.

What to do next: Continue to Remove SEC from Security Cloud Control

Remove an SEC from Security Cloud Control

This task removes an SEC (Secure Event Connector) from your Security Cloud Control management system when it is no longer needed or when troubleshooting connectivity issues.

Use this procedure when you need to disconnect and remove a Secure Event Connector from your Security Cloud Control environment. This is typically done during device decommissioning or when reconfiguring your security infrastructure.

Before you begin

See Secure event connector removal, on page 22.

Procedure

Step 1 Log in to Security Cloud Control.

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

Step 3 Select the row with the device type, **Secure Event Connector**.

Warning
Be careful NOT to select your Secure Device Connector.

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

Step 5 Click **OK** to confirm.

Continue to Remove a secure event connector from the secure device connector VM, on page 23.

The Secure Event Connector is successfully removed from Security Cloud Control and no longer appears in the connector list.

Remove a secure event connector from the secure device connector VM

Remove the Secure Event Connector from your Secure Device Connector virtual machine to complete the SEC removal process.

This is the second part of a two part procedure to remove the Secure Event Connector from your SDC. See Secure event connector removal, on page 22 before you begin.

Procedure

Step 1 Open your virtual machine hypervisor and start a console session for your SDC.

Step 2 Switch to the SDC user using the command **sudo su SDC**.

Example:

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

Step 3 Remove the SEC from the SDC virtual machine using one of the following commands:

- If you want to use the tenant selector (or if there's only one tenant on the VM):

  ```
  [sdc@tenant toolkit]$ sdc eventing delete
  ```

- If you want to specify the tenant directly in the command arguments:

  ```
  [sdc@tenant toolkit]$ sdc eventing delete CDO_{tenant-name}
  ```

Step 4 Confirm your intention to remove the SEC files.

The Secure Event Connector is successfully removed from the Secure Device Connector virtual machine.

Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS)

This task helps you identify the correct TCP, UDP, and NSEL ports that your Secure Event Connector (SEC) uses to receive events from your ASA or FDM-managed devices for Secure Logging Analytics (SaaS).

Secure Logging Analytics (SaaS) allows you to send events from your ASA or FDM-managed devices to certain UDP, TCP, or NSEL ports on the Secure Event Connector (SEC). The SEC then forwards those events to the Cisco cloud.

If these ports aren't already in use, the SEC makes them available to receive events and the Secure Logging Analytics (SaaS) documentation recommends using them when you configure the feature.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

If those ports are already in use, before you configure Secure Logging Analytics (SaaS), look at your SEC device details to determine what ports it is actually using to receive events.

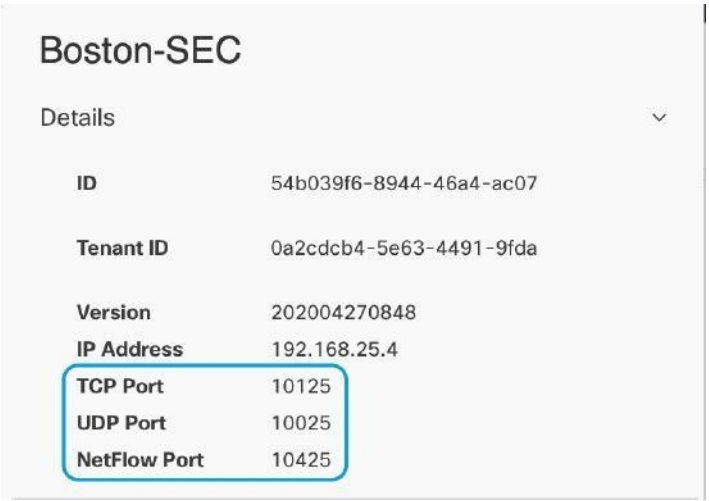
Follow these steps to find the port numbers the SEC uses:

Procedure

Step 1 From the left pane, click **Tools & Services** > **Secure ConnectorsAdministration** > **Secure ConnectorsAdministration** > **Integrations** > **Firewall Management Center** and then click the **Secure Connectors** tab.

Step 2 In the **Secure Connectors** page, select the SEC you want to send events to.

Step 3 In the **Details** pane, you will see the TCP, UDP, and NetFlow (NSEL) port you should send events to.



The Details pane displays the specific TCP, UDP, and NetFlow (NSEL) ports that your SEC is configured to use for receiving events from your devices.