

Onboard devices in Security Cloud Control Firewall Management

You can onboard both live devices and model devices to Security Cloud Control Firewall Management. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control Firewall Management.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control Firewall Management to the device or service.

This chapter covers the following sections:

- Introduction to Secure Connectors, on page 1
- Onboard devices in Security Cloud Control Firewall Management, on page 34
- Supported devices, software, and hardware for Security Cloud Control Firewall Management, on page 34

Introduction to Secure Connectors

A secure connector is a connector instance that runs in your network or supported cloud environment and provides a secure communication path between Security Cloud Control Firewall Management and managed resources. Secure connectors help Security Cloud Control Firewall Management manage devices that are not directly reachable from the internet and support event forwarding for logging and analytics workflows.

Use the **Secure Connectors** page to view, deploy, and manage connector instances for your tenant.

Secure connector types

The **Secure Connectors** page can include these connector types.

- Secure Device Connector (SDC): Provides a secure communication path between Security Cloud Control Firewall Management and supported managed devices.
- Secure Event Connectors (SEC): Receives events from supported devices and forwards the events to the Cisco cloud for logging and analytics.

About Secure Device Connector

A Secure Device Connector (SDC) is an intelligent proxy that lets Cisco devices communicate with Security Cloud Control Firewall Management when the devices are not directly reachable from the internet. When you onboard a device by using device credentials, you can deploy an SDC in your network to proxy communication between the device and Security Cloud Control Firewall Management.If the device is directly reachable from the internet, you can allow direct communication through the device's outside interface instead of using an SDC. The SDC performs these functions:

- Monitors Security Cloud Control Firewall Management for commands and messages for your managed devices.
- Executes commands on behalf of Security Cloud Control Firewall Management.
- Relays messages to your managed devices.
- Returns device responses.

Communication between the SDC and Security Cloud Control Firewall Management uses HTTPS with TLS 1.3 and AES-128-GCM. Credentials for onboarded devices and services are encrypted from the browser to the SDC and are encrypted at rest by using AES-128-GCM. Only the SDC has access to those credentials.

A user with the Super Administrator role is required to create a Secure Device Connector or a Secure Event Connector (SEC).

You can onboard these devices to Secure Device Connector through an SDC:

- Secure Firewall ASA
- FDM-Managed
- On-Premises Firewall Management Center using credentials method
- Meraki MX devices
- Generic SSH devices
- Cisco IOS devices

Secure Firewall Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center do not require an SDC and do not support onboarding through proxies. Ensure that these devices have proper DNS settings and outbound internet connectivity so they can connect to Cloud-Delivered Firewall Management Center.

Plan device connectivity

Security Cloud Control Firewall Management connects to managed devices either through the cloud connector or through an SDC.

Table 1:

Connection method	Use when	Required network access
Direct cloud connector	The device is directly reachable from the internet.	Allow inbound access from the Security Cloud Control Firewall Management IP addresses for your cloud region on port 443, or on the port that you use for device management.
SDC	The device is not directly reachable from the internet, or the source explicitly requires an on-premises SDC.	Allow full inbound access from the SDC host on port 443, or on the port that you use for device management. Ensure that the SDC VM can reach the device management interface.

An FDM-managed device can be onboarded to Security Cloud Control Firewall Management by using device credentials, a registration key, or its serial number whether it is directly accessible from the internet. If the device does not have direct internet access, but it resides on a network that does, the Security Services Exchange connector that is delivered as part of the device can reach the Security Services Exchange cloud and allow the FDM-managed device to be onboarded.

The source explicitly states that you need an on-premises SDC to onboard the following:

- An ASA device that is not accessible from the cloud
- An FDM-managed device that is not accessible from the cloud when you use the credentials onboarding method
- A Cisco IOS device
- A device with SSH access
- An On-Premises Firewall Management Center using its credentials for Government customers.

All other devices and services do not require an on-premises SDC because Security Cloud Control Firewall Management connects by using its cloud connector.

Docker network considerations for the SDC

SDC runs as a Docker container. Docker commonly uses the `172.17.0.0/16` subnet for the default bridge network, docker0.

If `172.17.0.0/16`, or any part of the Docker-assigned network space, overlaps with your existing network IP space, change the Docker network defaults before deploying the SDC. To use alternate networks, edit /etc/docker/daemon.json configuration.

For example, Use the supernet `10.198.0.1/24` for Docker networking address pools and use IP address `10.198.128.0/17` as the default docker bridge interface, docker0, from the subnet `10.198.0.0/24`.

```
sudo vi /etc/docker/daemon.json

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

```
    "max-size": "100m",
    "max-file": "5"
  },
    "bip": "10.198.0.1/24",
    "default-address-pools": [
        {
            "base": "10.198.128.0/17",
            "size": 24
        }
    ]
}

(save and exit)

sudo reboot (required)
```

For more information, see Networking overview.

Allow inbound access for direct cloud connectivity

Security Cloud Control connects to the devices that it manages through the cloud connector or through an (SDC).

When you connect Security Cloud Control Firewall Management directly to a device through the cloud connector, allow inbound access on port 443, or on the port that you have configured for device management, from the IP addresses for your region.

Table 2:

Region	URL	Allow inbound access from
Asia-Pacific-Japan (APJ)	https://security.cisco.com	54.199.195.111, 52.199.243.0
Australia (AUS)	https://security.cisco.com	13.55.73.159, 13.238.226.118
Europe, Middle East, and Africa (EMEA)	https://security.cisco.com	35.157.12.126, 35.157.12.15
India (IN)	https://security.cisco.com	35.154.115.175 13.201.213.99
United States (US)	https://security.cisco.com	52.34.234.2 52.36.70.147

Special Consideration for Connecting an ASA to an SDC

Specifically, for ASA the SDC uses the same secure communications channel used by ASDM.

If the ASA under management is also configured to accept AnyConnect VPN Client connections, the ASDM HTTP server port must be changed to a value of 1024 or higher. Note that this port number will be the same port number used when onboarding the ASA device into Security Cloud Control.

Example ASA Commands

The following examples assume that the ASA outside interface is named 'outside' and an AnyConnect client is configured on the ASA so the ASDM HTTP server is listening on port 8443.

To enable the outside interface, enter these commands:

Asia-Pacific-Japan Region:

- http 54.199.195.111 255.255.255.255 outside
- http 52.199.243.0 255.255.255.255 outside

Australia Region

- http 13.55.73.159 255.255.255.255 outside
- http 13.238.226.118 255.255.255.255 outside

EMEA Region

- http 35.157.12.126 255.255.255.255 outside
- http 35.157.12.15 255.255.255.255 outside

India Region

- http 35.154.115.175 255.255.255.255 outside
- http 13.201.213.99 255.255.255.255 outside

United States Region

- http 52.34.234.2 255.255.255.255 outside
- http 52.36.70.147 255.255.255.255 outside

To enable the ASDM HTTP server port, in the case where AnyConnect VPN Client is in use, enter this command:

http server enable 8443

Plan SDC capacity and host requirements

Each Security Cloud Control Firewall Management organization can have an unlimited number of SDCs. An SDC belongs to one organization only and is not shared across organizations.For deployment planning, one SDC is expected to support approximately 500 devices. Actual capacity depends on the features enabled on those devices and the size of their configuration files.

Deploying more than one SDC lets you:

- Scale device management without performance degradation.
- Place SDCs in isolated network segments while keeping the devices in the same Security Cloud Control Firewall Management organization.
- Run multiple SDCs on one host by following the bootstrap procedure for each additional SDC.

The first SDC name includes the tenant name and the number 1. Each additional SDC is numbered in sequence.

Deploy a VM for Running the Secure Device Connector and Secure Event Connector

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are nonperimeter based and do not have a public IP address, or have an open port to the outside interface.

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

The number of devices a single SDC can manage depends on the features that are implemented on those devices and the size of their configuration files. To plan your deployment, however, we expect one SDC to support approximately 500 devices. For more information, see Using Multiple SDCs on a Single Security Cloud Control Tenant.

This procedure describes how to install an SDC in your network, using Security Cloud Control's VM image. This is the recommended and most reliable way to create an SDC.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support Web or Content Proxy inspection between the Secure Device Connector (SDC) and the internet. If using a proxy server, disable inspection for traffic between the SDC and Security Cloud Control.
- The SDC must have full outbound access to the internet on TCP port 443, or the port you have configured for device management.
- The devices that are managed by Security Cloud Control must allow inbound traffic from the SDC VM's IP address.
- Review Connect Allow inbound access for direct cloud connectivity , on page 4 to the Secure Device Connector to ensure proper network access.
- If you are using a proxy on your network, ensure that you have all the required details before running the host setup command. Most of the issues are related to incorrect proxy configurations. Important details are:
  - The IP/hostname of your proxy.
  - Whether or not your proxy intercepts traffic and reencrypts it using its own cert. This detail is the cause of most of the complications with the SDC VM setup.
    - If your proxy does intercept traffic, have the root certificate ready when configuring the VM. You can paste it in when prompted so that the host and the SDC know to trust the certificates generated by your proxy.
    - If your proxy does not intercept traffic, then nothing else is required here.
  - The following items are most likely the same for proxied HTTP and HTTPS connections. However, if you use a different proxy for each protocol, you would need all of the following for each:
    - The IP address of your proxy
    - The port your proxy uses

- Whether your proxy requires that the connection to the proxy itself be over HTTPS (typically not the case). For example, if the address of your proxy is listed as https://proxy.corp.com:80 then you would answer yes. If the listed address is http://proxy.corp.com:80 then you would answer no. Note that both URLs use port 80, but the protocol is different.
- The authentication details of your proxy including:
  - Whether your proxy requires auth (most do not)
  - If yes, then you'll need the username and password available when you configure the host.

Supported Installations

- Security Cloud Control supports installing its SDC VM OVF image using the vSphere web client or the ESXi web client.
- Security Cloud Control does not support installing the SDC VM OVF image using the vSphere desktop client.
- Security Cloud Control supports installing the SDC on your own Ubuntu instance. Versions 20LTS - 24LTS are currently supported.
- ESXi 5.1 hypervisor.

System Requirements

- System requirements for a VM with one SDC:
  - 2 vCPUs
  - 2 GB of memory
  - 64 GB of disk space
- Each SDC you add to your host requires an additional 1 vCPU and 1 GB of RAM.
- System requirements for a VM with one SEC (a component that is used in Cisco Security Analytics and Logging):
  - 4 vCPUs minimum
  - 8 GB of memory
- Each SEC you add to the host requires doubling its resources, therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:
  - 6 vCPUs
  - 10 GB memory
  - 64 GB of disk space

Prepare for Installation

- To configure networking manually on the host, gather the following information:
  - The static IP address that you want to use for your VM
  - The passwords to use for the `cdo`user (or whichever user has sudo access) and the sdc user (the user under which Docker runs)
  - 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/NTP server
- The SDC virtual machine is configured to install security patches regularly and to do this, opening port 80 outbound is required.

  If your network is using allow/deny lists for outbound connections, you need to allow connections to ubuntu.com so those security updates can be applied.



Note Ubuntu secures its updates with checksums and only uses HTTP, not HTTPS. To pull security updates, you must allow HTTP connections to ubuntu.com.

Deploy the VM

There are two options for deploying the VM used to run the SDC and SEC.

1. Follow the steps below to download the VMware image provided by Security Cloud Control.
2. To deploy Ubuntu 20, 22, or 24 yourself. If deploying your own Ubuntu instance, you may skip the following section and proceed to the Configure the VM section.

Procedure

1. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
2. Select the **Secure Connectors** tab on the **Services** page, click the blue plus button, and select **Secure Device Connector**.
3. Click **Download the SDC VM** image. This opens in a new tab.
4. Extract all the files from the .zip file. They look similar to these:
   - CDO-SDC-VM-ddd50fa.ovf
   - CDO-SDC-VM-ddd50fa.mf
   - CDO-SDC-VM-ddd50fa-disk1.vmdk
5. Log in to your VMware server as an administrator using the vSphere Web Client.

Note Do not use the ESXi Web Client.

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

6. When the setup is complete, power on the SDC VM.
7. Open the console for your new SDC VM.
8. Log in with the `cdo` username. The default password is `adm123`.

Configure the VM

Now you are able to bring up the console for the VM image you deployed (or SSH into it if you rolled your own and enabled SSH), you should run the configuration script to get your host ready to run the SDC or SEC Docker container(s).

1. If you downloaded the Security Cloud Control-provided VM, the CLI is already installed, and you can proceed to step 2. If you have deployed your own VM, SSH into it and run the command to install the CLI:

   ```
   curl -O
   https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
    && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
   ```

2. Start the host configuration by running the command:

   ```
   sudo sdc host configure
   ```

3. When prompted for the password, enter adm123 for the Security Cloud Control-provided VM or whatever admin password you chose for your own VM.
4. Follow the prompts to configure the `sdc` user.
5. When prompted for the networking configuration, choose one of the following:
   - Manually configure this host with a static IP: If you want to specify the IP, gateway, DNS server, and so on, for this host and write it to the system config on the VM.
   - DHCP: If you have a DHCP server assigning static IPs to your VMs.
   - Static IP is already configured and I don't want to change my networking now.
6. When prompted, answer the questions about your proxy configuration. Review the detailed list at the top of this topic for all the prerequisites and potential proxy configuration options.
7. If you have configured a proxy, you will be prompted to reboot the VM for all the proxy settings to take effect. If you did not, you will not be prompted to reboot and you can move on to step 8.
8. Set a custom internet access test URL. You only need to do this if you deny all outbound connections by default. If you do, then specify a publicly accessible web url such at https://google.com that is on your allow list.
9. Install the latest security patches, some requires os tools and Docker server.
10. When prompted, indicate whether you want to have the script harden your SSH configuration.

If using our VM, proceed. If you are using your own VM and configuring SSH yourself, you may want to skip this step to avoid changing your current configuration.

11. When prompted to enable automatic updates for the SDC or SEC and the CLI itself, it is recommended that you do this to stay up to date with bug fixes, patches, and new features. If your policies prevent you from allowing automatic updates, see Update your Secure Device Connector.

Deploy a Secure Device Connector On Your VM

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

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

The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices. See Use multiple Secure Device Connectors on one tenant , on page 23 for more information.

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

Note The preferred, easiest, and most reliable way to install an SDC is to download Security Cloud Control's SDC OVA image and install it.

Before you begin

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

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

- ESXi 5.1 hypervisor.

- Ubuntu 22.04 and Ubuntu 24.04 operating system.
- System requirements for a VM with only an SDC:
  - VMware ESXi host needs 2 CPUs.
  - VMware ESXi host needs a minimum of 2 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice. This value assumes you are using Logical Volume Management (LVM) with the partition so you can expand required disk space as needed.
- System requirements for a VM with an SDC and **a single** Secure Event Connector (SEC) for your tenant. (The SEC is a component used in Cisco Security Analytics and Logging).

  Each SEC you add to the VMware ESXi host requires an additional 4 CPUs and an additional 8 GB of memory.

  Therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:
  - VMware ESXi host needs 6 CPU.
  - VMware ESXi host needs a minimum of 10 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice.
- After you have updated the CPU and memory on the VM, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.
- Users performing this procedure should be comfortable working in a Linux environment and using the vi visual editor for editing files.
- If you are installing your on-premise SDC on a CentOS virtual machine, we recommend you install Yum security patches on a regular basis. Depending on your Yum configuration, to acquire Yum updates, you may need to open outbound access on port 80 as well as 443. You will also need to configure yum-cron or crontab to schedule the updates. Work with your security-operations team to determine if any security policies need to change to allow you to get the Yum updates.



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

Procedure

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

Step 2 In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.

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

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

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

- 8GB of RAM
- 10GB disk space

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

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

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

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

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

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

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

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

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

Note
Use the "Install using the repository" method.

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

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

Step 14 Create two users: `cdo` and `sdc`. Use the `cdo` user to perform administrative tasks without directly accessing the root user. The `sdc` user will be designated for running the SDC docker container.

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

Step 15 Set a password for the `sdc` user.

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

Step 16 Add the `sdc` user to the `wheel` group to give it administrative (sudo) privileges.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 24 Download the bootstrap bundle from Security Cloud Control.

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

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

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

The SDC should now show "Active" in Security Cloud Control.

Bootstrap a Secure Device Connector on the Deployed Host

Procedure

Step 1 In the left pane, click **Admin** > **Secure Connectors**.

Step 2 In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.

Step 3 On the **Services** page, select the **Secure Connectors** tab, click the + icon, and select **Secure Device Connector**.

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

Step 5 SSH into your VM using the admin user, typically `cdo`, and your chosen password.

Step 6 Switch to the `sdc` user using the command:

```
sudo su - sdc
```

Step 7 Bootstrap your new SDC using the command:

```
sdc bootstrap <paste-your-bootstrap-data-here>
```

Step 8 Select the version of the SDC you want to use.

We have three options for the SDC version:

- SDC 2024- This is the version that most will want to run.
- SDC 2024 with FIPS enabled- Choose this version if you are subject to FedRamp compliance.
- SDC Legacy- This version is no longer receiving feature updates and it is recommended to run SDC 2024 instead.

Step 9 The CLI pulls the container image and starts the SDC and you can validate that your SDC is active and operational on the user interface, and also on the host by running:

```
sdc show running
```

You should now see an SDC for your tenant.

Deploy a Secure Device Connector to vSphere Using Terraform

Before you begin

This procedure details how you can use the Security Cloud Control SDC Terraform module for vSphere in conjunction with the Security Cloud Control Terraform Provider to deploy an SDC to your vSphere. Ensure you review the following prerequisites before attempting to perform this task procedure:

- You have vSphere datacenter version 7 and above
- You have an admin account on the datacenter with permissions to do the following:
  - Create VMs
  - Create folders
  - Create content libraries
  - Upload files to content libraries
- Terraform knowledge

Procedure

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

Step 2 Configure the Security Cloud Control Terraform provider in your Terraform repository by following the instructions in Security Cloud Control Terraform Provider.

Example:

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

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

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

Example:

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

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

Step 4 Write Terraform code to create the SDC in vSphere using Security Cloud Control_sdc Terraform module.

Example:

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

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

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

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

See the Security Cloud Control Automation Repository in the CiscoDevNet for a complete example.

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

```
sdc host status
```

Depending on the readout, you may need to manually run:

```
sdc host configure
```

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

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

Before you begin

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

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the SDC and the Internet. If using a proxy server, disable inspection for traffic between the Secure Device Connector (SDC) andSecurity Cloud Control.
- See Connect Security Cloud Control to the Secure Device Connector to ensure proper network access.
- You require an AWS account, an AWS VPC with at least one subnet, and an AWS Route53-hosted zone.
- Ensure you have the Security Cloud Control bootstrap data, your AWS VPC ID, and its subnet ID handy.
- Ensure that the private subnet to which you deploy the SDC has a NAT gateway attached.
- Open traffic on the port on which your firewall management HTTP interface is running, from your firewalls to the Elastic IP attached to the NAT gateway.

Procedure

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

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

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

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

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

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

What to do next:

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

Note

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

Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine

Security Cloud Control's on-premises Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to this point. Since CentOS 7 is now end-of-life and has been deprecated by Security Cloud Control, we have created this migration process to help you migrate all SDCs from CentOS 7 to an Ubuntu virtual machine.

Before You Migrate

- The SDC must have full outbound access to the internet on TCP port 443.
- The Ubuntu virtual machine running the SDC must have network access to the management interfaces of the devices it communicates with, such as ASAs and Cisco IOS devices.
- Any networking rules created for the IP address or FQDN of the old SDC VM to reach your devices should be recreated with the IP address or FQDN of the new SDC VM.
- The migration will take 10 to 15 minutes. During this time, your device will continue to enforce security policy and route network traffic, but you will not be able to communicate with it through the SDC.

Prerequisites

Deploy a new host by following the instructions on Deploy a VM for Running the Secure Device Connector and Secure Event Connector.

Host Configuration

Follow this procedure if you are migrating the SDC and/or SEC:

1. Download the new VM image here.
2. Unzip the CDO-SDC_VM.zip file. You should see three VM files named similarly to the following:
   - CDO-SDC-VM-708cd33-2024-05-30-2031-disk1.vmdk
   - CDO-SDC-VM-708cd33-2024-05-30-2031.mf
   - CDO-SDC-VM-708cd33-2024-05-30-2031.ovf
3. Deploy the VM you just downloaded.
4. Note the static IP address or FQDN you assigned to the new VM.
5. Using SSH, log in to the new VM as the `cdo` user.
6. At the prompt, enter the command:

   ```
   sudo sdc host configure
   ```

Note

- Follow the prompts in the migration script closely. The script is well-documented and will guide you through the migration process, explaining each step.
- At the end of the migration script, you will receive a message indicating that your SDC has been migrated to the new VM. The SDC will retain its name after the migration.

SDC Migration

Procedure:

1. Using SSH, log in to the old (CentOS) SDC as the `cdo` user.
2. Install the CLI using the command:

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
```

3. Run the following command and follow the prompts:

```
sudo sdc migrate now
```

Verification:

1. Log in to your Security Cloud Control tenant.
2. In the left pane, click **Tools & Services** > **Secure Connectors**.
3. Select the SDC you migrated, and in the **Actions** pane, click **Request Heartbeat**.

Note Ensure that the SDC is in the **Active** state.

SEC Migration

Procedure:

1. Using SSH, log in to the old (CentOS) SDC as the `cdo` user.
2. Install the CLI using the command:

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
```

3. Run the following command and follow the prompts:

```
sudo sdc eventing migrate
```

4. You can configure your devices to point to the new IP address of the SEC or you can shut down the old host and assign the new host the same IP address that the old host had so that the devices do not need to be updated.

Verification:

For information on the state of the SEC, see Use Health Check to Learn the State of your Secure Event Connector.

Additional Instructions

Do Not Restart Your Old SDC

After the migration is complete, do not restart your old SDC on the original virtual machine.

Revert Failed Migration

If the migration fails for any reason, or the result is not what you are expecting and you want to revert to the old SDC, follow the instructions below:

1. Log in to the new VM and switch to the **SDC** user.
2. Ensure the SDC is not currently running on the new VM using the command:

   ```
   docker ps
   ```
3. If the SDC is running, run the command:

   ```
   sdc stop
   ```
4. Confirm that the SDC has stopped running by executing `docker ps` again.
5. Log in to the old VM and run the command:

   ```
   sdc migrate revert
   ```
6. When the old SDC is active and visible in the UI, return to the new VM and execute the command:

   ```
   sdc delete <your-tenant-name-here>
   ```
7. Refresh the browser completely, click on the SDC, and verify that the IP of the old host appears in the sidebar.

   If the new IP still appears despite following these steps, request a new health check, refresh the browser, and check again.
8. To revert the SEC migration,run the command:

   ```
   sdc eventing revert
   ```

Change the IP Address of a Secure Device Connector

Before you begin

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

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

Procedure

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

Step 2 To view your SDC VM's network interface configuration information before changing the IP address, use the command:

```
[cdo@localhost ~]$ ip addr
```

Step 3 To change the IP address of the interface, re-initiate the host configuration using the command:

```
[cdo@localhost ~]$ sdc host configure network
```

Step 4 Enter your password at the prompt.

Step 5 The configure script will then ask you about your networking configuration, write the new config file with the new IP and apply that configuration.

Note
You will lose your SSH connection at this time.

Step 6 Create an SSH connection using the new IP address you assigned to your SDC and log in.

Step 7 Your SDC should start automatically, but if it does not, run the following commands:

```
[cdo@localhost ~]$ sudo su - sdc
```

```
[cdo@localhost ~]$ sdc start
```

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

Step 8 You can also check your SDC's connectivity through the Security Cloud Control user interface. To do that, open the Security Cloud Control application and navigate to **Tools & Services** > **Secure Connectors Administration** > **Integrations** > **Secure Connectors** page.

Step 9 Refresh the page once and select the secure connector whose IP address you changed.

Step 10 On the **Actions** pane, click **Request Heartbeat**. You should see the **Heartbeat** requested successfully message, and the **Last Heartbeat** should display the current date and time.

Move an ASA from one Secure Device Connector to Another

Procedure

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

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

Step 3 Click the **ASA** tab.

Step 4 Select the ASA or ASAs you want to move to a different SDC.

Step 5 In the **Device Actions** pane, click **Update Credentials**.

Step 6 Click the Secure Device Connector button and select the SDC you want to move the device to.

Step 7 Enter the administrator username and password Security Cloud Control uses to log into the device and click **Update**. Unless they were changed, the administrator username and password are the same credentials you used to onboard the ASA. You do not have to deploy these changes to the device.

Note
If all the ASAs use the same credentials, you can move ASAs in bulk from one SDC to another. If the ASAs have different credentials, you have to move them from one SDC to another one at a time.

Rename a Secure Device Connector

Procedure

Step 1 In the left pane, choose **Administration** > **Integrations** > **Secure Connectors**.

Step 2 Select the SDC you want to rename.

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

Step 4 Rename the SDC.

This new name will appear wherever the SDC name appears in the Security Cloud Control interface including the Secure Device Connectors filter of the **Security Devices** pane.

Specify a default Secure Device Connector

When you onboard devices that connect to Security Cloud Control Firewall Management through an SDC, they are associated with the default SDC for your tenant unless you specify another SDC during onboarding.

You can specify which SDC is selected by default on the Secure Connectors page:

Procedure

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

Step 2 Select the SDC that you want to be the default.

Step 3 In the Actions pane, click **Make Default**. If you don't see the Make Default action, then the SDC already is the default SDC.

Update a Secure Device Connector manually

Use this task as a troubleshooting tool. The source says that the SDC is usually updated automatically and that you should not need to perform a manual update unless errors occur.

Procedure

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

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

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

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

Step 4 Upgrade the SDC:

```
sdc upgrade
```

Note
Recommended updates and maintenance on the SDC Virtual Machine

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

Use multiple Secure Device Connectors on one tenant

You can install an unlimited number of SDCs on a tenant. Multiple SDCs let you manage more devices and place connectors in different network segments while keeping those devices in the same Security Cloud Control Firewall Management tenant.The procedure for deploying a second or later SDC is the same as the procedure for the first SDC.The first SDC name includes the tenant name and the number `1`. Each additional SDC is numbered in order.

- The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC.
- The initial SDC for your tenant incorporates the name of your tenant and the number 1. Each additional SDC is numbered in order.

Find devices that sse the same Secure Device Connector

Follow this procedure to find devices that connect through the same SDC:

Procedure

Step 1 In the left pane, **Security Devices**.

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

Step 3 Click the **Devices** tab to locate the device.

Step 4 Click the appropriate device type tab.

Step 5 If there is any filter criteria already specified, click the **clear** button at the top of the **Security Devices** page to show all the devices and services you manage with Security Cloud Control.

Step 6 In the **Secure Device Connectors** section of the filter, check the name of the SDC(s) you're interested in. The **Security Devices** page displays only the devices that connect to Security Cloud Control through the SDC you checked in the filter.

Step 7 (Optional) Check additional filters in the filter menu to refine your search further.

Step 8 (Optional) When you're done, click the **clear** button at the top of the **Security Devices** page to show all devices and services you manage with Security Cloud Control.

Remove a Secure Device Connector

Deleting an SDC is not reversible. After you remove it, you cannot manage the devices that were connected to that SDC until you install a new SDC and reconnect the devices. Reconnecting devices can require you to enter administrator credentials again.

Before you remove an SDC, move the connected devices to another SDC or remove them from Security Cloud Control Firewall Management.

Procedure

Step 1 Remove any devices connected to the SDC you want to delete. You can do this one of two ways:

- Remove from Security Cloud Control any devices connected to the SDC you want to delete.
  - **a.** See Find all Devices that Connect to Security Cloud Control Using the Same SDC to identify all the devices used by the SDC.
  - **b.** In the **Security Devices** page, select all the devices you identified.
  - **c.** In the Device Actions pane, click **Remove** and click **OK** to confirm your action.

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

Step 3 In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.

Step 4 On the **Services** page with the **Secure Connectors** tab selected, click the blue plus button and select **Secure Device Connector**.

Step 5 In the Secure Connectors table, select the SDC you want to remove. Its device count should now be zero.

Step 6 In the Actions pane, click **Remove**. You receive this warning:

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

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

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

Step 7 In the confirmation dialog box, if you wish to proceed, enter your SDC's name as it is stated in the warning message.

Step 8 Click **OK** to confirm the SDC removal.

Open source and third-party license in SDC

==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

This package, "amqplib", is licensed under the MIT License. A copy maybe found in the file LICENSE-MIT in this directory, or downloaded from

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** bluebird ***

The MIT License (MIT)

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the 'Software'), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** command-line-args ***

The MIT License (MIT)

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** ip ***

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

Permission is hereby granted, free of charge,to any person obtaining a copy of this software andassociated documentation files (the "Software"), todeal in the Software without restriction, includingwithout limitation the rights to use, copy, modify,merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whomthe Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission noticeshall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FORANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stable-stringify ***

This software is released under the MIT license:

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS ORCOPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHERIN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR INCONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/>

Based on Underscore.js, copyright Jeremy Ashkenas,

DocumentCloud and Investigative Reporters & Editors<http://underscorejs.org/>

This software consists of voluntary contributions made by manyindividuals. For exact contribution history, see the revision historyavailable at https://github.com/lodash/lodash

The following license applies to all parts of this software except as

documented below:

====

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

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

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

====

Copyright and related rights for sample code are waived via CC0. Samplecode is defined as all source code displayed within the prose of thedocumentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externallymaintained libraries used by this software which have their ownlicenses; we recommend you read them, as their terms may differ from theterms above.

==========

*** log4js ***

Copyright 2015 Gareth Jones (with contributions from many other people)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions andlimitations under the License.

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

This project is free software released under the MIT/X11 license:

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

*** Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.**

*** Redistributions in binary form must reproduce the above copyrightnotice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.**

*** Neither the name of Digital Bazaar, Inc. nor thenames of its contributors may be used to endorse or promote productsderived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" ANDANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AREDISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANYDIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED ANDON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THISSOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

*** request ***

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display

generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT License - http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

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

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

==========

*** when ***

Open Source Initiative OSI - The MIT License

http://www.opensource.org/licenses/mit-license.php

Copyright (c) 2011 Brian Cavalier

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

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

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Onboard devices in Security Cloud Control Firewall Management

You can onboard both live devices and model devices to Security Cloud Control Firewall Management. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control Firewall Management.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control Firewall Management to the device or service.

This chapter covers the following sections:

Supported devices, software, and hardware for Security Cloud Control Firewall Management

Security Cloud Control Firewall Management is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms.

This section describes the supported device types, software, hardware, and constraints for managing firewall, cloud, SD-WAN, Cisco IOS, Cisco Umbrella, and management center integrations in Security Cloud Control Firewall Management.

Support scope

Security Cloud Control Firewall Management is a cloud-based management solution for security policies and device configurations across multiple security platforms. The source identifies support for these management areas:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center, on-premises

Security Cloud Control Firewall Management documentation identifies the devices, software, and hardware that Security Cloud Control Firewall Management supports. If the documentation does not explicitly claim support for a software version or device type, Security Cloud Control Firewall Management does not support it.

Cisco Secure Firewall ASA

Cisco Adaptive Security Appliance (ASA) is a security device that integrates firewall, VPN, and intrusion prevention capabilities. Security Cloud Control supports ASA device management to streamline configuration management and support regulatory compliance across the network infrastructure.

Cisco Secure Firewall Threat Defense

Cisco Secure Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It includes security functions such as intrusion prevention, application control, URL filtering, and advanced malware protection.

A Secure Firewall Threat Defense device can be deployed on ASA hardware appliances, Cisco firewall hardware appliances, and virtual environments. You can manage threat defense devices through management interfaces such as Cisco Firewall Management Center, Security Cloud Control, and Firewall Device Manager.

Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It offers comprehensive security functions, including intrusion prevention, application control, URL filtering, advanced malware protection, and so on. An FTD can be deployed on ASA hardware appliances, and Cisco firewall hardware appliances, and in virtual environments. Managing threat defense devices is possible through various management interfaces, such as Cisco Firewall Management Center and Security Cloud Control

For more information on software and hardware compatibility, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Cisco Secure Firewall Management Center

Security Cloud Control Firewall Management simplifies the management of on-premises Firewall Management Center by establishing a secure integration, discovering security devices, and enabling centralized policy management. Security policies such as firewall rules, VPN settings, and intrusion prevention policies can be efficiently managed and deployed across all devices under FMC.

ASA support specifics

Security Cloud Control Firewall Management support for ASA has these constraints:

- Security Cloud Control Firewall Management can manage all ASA platforms that run currently supported code versions, including ASAv instances.
- Security Cloud Control Firewall Management does not support ASA Services Module (ASASM).
- Security Cloud Control Firewall Management does not test end-of-life ASA code versions and does not recommend them for production.
- Use currently supported ASA code versions for optimal results.
- ASA 8.3 is not supported with the new policy view.
- Security Cloud Control Firewall Management does not manage the ASA FirePOWER module because the module runs a different operating system from ASA. Manage the ASA FirePOWER module separately with Secure Firewall Management Center or ASDM.
- End-of-life code and hardware might continue to work with Security Cloud Control Firewall Management. Because end-of-life code and hardware are not part of Security Cloud Control Firewall Management testing, correct operation with end-of-life software and hardware is not guaranteed or assured.

Refer to the version download page for Cisco "suggested release" or "gold star" versions.

- ASA versions 8.x, 9.1, and 9.2 do not support TLS 1.2 on the management plane and are considered insecure for ASA software management.

For a full discussion of ASA, ASDM, and hardware compatiblity, see the Cisco Secure Firewall ASA Compatibility guide.

Secure Firewall Threat Defense Device Support Specifics

Secure Firewall Threat Defense is Cisco's next generation firewall. It can be installed on a variety of hardware and virtual platforms; see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Firewall Threat Defense with Secure Firewall Device Manager

You can add Security Cloud Control managment to threat defense Version 6.4+ with Firewall Device Manager. However, this option is only available upon request for those who already have device manager support enabled on their tenant. See:

- Open a Support Ticket with TAC to request this option.

Snort

Snort 3 is the default inspection engine for threat defense starting in threat defense Version 6.7 (with device manager) and Version 7.0 (with management center).



Important If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

Cloud Device Support Specifics

The following table describes software and device type support for cloud-based devices. Read the affiliated links for more information about onboarding and feature functionality for the device types in the table below:

Devices Types	Notes
Google Cloud Platform	Google Cloud Platform (GCP) receives updates through the GCP console. Refer to Google Cloud documentation for more information about the platform and available services.
Microsoft Azure	Azure receives updates through the Azure console. Refer to Azure documentation for more information about the platform and available services.