

Onboard Secure Firewall ASA

This chapter explains the various different methods using which a Secure Firewall ASA can be onboarded.

- Onboard Secure Firewall ASA, on page 1
- Onboard ASA device to Security Cloud Control Firewall Management, on page 1
- Onboard a high availability pair of ASA devices to Security Cloud Control Firewall Management, on page 3
- Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management, on page 4
- Onboard multiple ASAs to Security Cloud Control Firewall Management, on page 5
- Create and import an ASA model to Security Cloud Control Firewall Management, on page 7
- Configuration import for offline device management, on page 8

Onboard Secure Firewall ASA

This chapter explains the various different methods using which a Secure Firewall ASA can be onboarded.

Onboard ASA device to Security Cloud Control Firewall Management

This task connects a single live ASA device to Security Cloud Control Firewall Management for centralized management and monitoring.

Use this procedure to onboard a single live ASA device, not an ASA model, to Security Cloud Control Firewall Management. If you want to onboard multiple ASAs at once, refer to Onboard ASAs in Bulk.

Before you begin

Device Prerequisites

- The device must be running version 8.4 or later.

Note TLS 1.2 became available for the ASA management plane in version 9.3(2). To onboard to Security Cloud Control Firewall Management using version 9.3(2), a local SDC is required.

- The running configuration file of your ASA must be less than 4.5 MB.
- IP addressing: Each ASA, ASAv, or ASA security context must have a unique IP address, and the SDC must connect to it on the interface configured to receive management traffic.

Certificate Prerequisites

If your ASA device does not have a compatible certificate, onboarding the device may fail. Make sure that these requirements are met:

- The device must use TLS version 1.0 or later.
- The certificate presented by the device must not be expired, and its issuance date must be in the past. This means the certificate is already valid and not scheduled to become valid later.
- The certificate must be a SHA-256 certificate. SHA-1 certificates are not accepted.
- One of the following conditions must be met:
  - The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.
  - The device uses a certificate signed by a trusted Certificate Authority (CA) and provides a certificate chain that links the presented leaf certificate to the relevant CA.

Open SSL Cipher Prerequisites

If the device does not have a compatible SSL cipher suite, it cannot successfully communicate to the Secure Device Connector (SDC). Use any of these cipher suites:

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

Procedure

Step 1 Choose Security Devices.

Step 2 Click the **Onboard device or service** ( ) icon.

Step 3 Click the **ASA** tile.

Step 4 In the **Locate Device** step, perform these actions:

a. Enter a name for the device.

b. Enter the location of the device or service (IP address, FQDN, or URL). The default port is 443.

c. Click **Next**.

Step 5 In the **Credentials** step, enter the username and password of the ASA administrator, or similar highest-privilege ASA user, that Security Cloud Control Firewall Management will use to connect to the device and click **Next**.

Step 6 After labeling your device or service, you can view it in the **Security Devices** list.

Note
Analyzing the configuration may take some time, depending on its size and the number of devices or services.

The ASA device is successfully onboarded and appears in the **Security Devices** list, where you can manage and monitor its configuration.

Onboard a high availability pair of ASA devices to Security Cloud Control Firewall Management

A high availability ASA device onboarding process is a network management approach that

- requires onboarding only the primary ASA to Security Cloud Control Firewall Management
- uses the failover link to manage the secondary ASA automatically, and
- eliminates the need to onboard the secondary device separately.

Additional onboarding information

For more information about onboarding ASA devices to Security Cloud Control Firewall Management, refer to Onboard ASA device to Security Cloud Control Firewall Management, on page 1.

Secure Firewall ASA multi-context mode onboarding to Security Cloud Control Firewall Management

ASA multi-context mode onboarding is a process that

- partitions a single ASA into multiple logical devices known as contexts
- onboards each security context and admin context as a separate ASA in Security Cloud Control Firewall Management, and
- manages each context as if it were a separate ASA device.

Multi-context mode configuration types

The three types of configurations used in an ASA configured in multi-context mode are:

- Security context
- Admin context
- System configuration

Security contexts:

Each security context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple security contexts are similar to having multiple standalone devices. A security context is not a virtual ASA in the sense of a virtual machine image installed in a private cloud infrastructure. A security context is configured on an ASA that is installed on a hardware appliance. Each context is configured on a physical interface of that appliance.

For more information about multi-context mode, refer to ASA CLI and ASDM configuration guides.

Security Cloud Control Firewall Management onboards each security context as a separate ASA and manages it as if it were a separate ASA.

Admin contexts:

The admin context is similar to a security context, except that when a user logs in to the admin context, the user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way and can be used as a regular context. However, because logging into the admin context grants administrator privileges over all contexts, access to the admin context should be restricted to authorized users.

Security Cloud Control Firewall Management onboards each admin context as a separate ASA and manages it as if it were a separate ASA. Security Cloud Control Firewall Management also uses the admin context when upgrading ASA and ASDM software on the appliance.

System configuration:

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and setting other context operating parameters within the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself. When the system needs to access network resources, such as downloading the contexts from the server, it uses one of the contexts designated as the admin context.

Security Cloud Control Firewall Management does not onboard the system configuration.

Onboard prerequisites for security and admin contexts:

Before you onboard security or admin contexts, check the prerequisites in Onboard ASA device to Security Cloud Control Firewall Management, on page 1.

To learn which Cisco appliances support ASAs in multi-context mode, refer to the "Multiple Context Mode" chapter in the *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide* for your ASA software version.

An ASA running as a single context firewall, or as the admin context of a multiple-context firewall, can use different port numbers for ASDM and Security Cloud Control Firewall Management access. ASA security contexts use a fixed port (port 443) for ASDM and Security Cloud Control Firewall Management access.

Onboard ASA security and admin contexts:

To onboard a security context or admin context, follow the instructions in Onboard ASA device to Security Cloud Control Firewall Management, on page 1 or Onboard multiple ASAs to Security Cloud Control Firewall Management, on page 5.

Upgrade security contexts:

Security Cloud Control Firewall Management treats each security and admin context of a multiple-context ASA as a separate ASA and each is onboarded separately. However, all security and admin contexts of a multiple-context ASA run the same version of ASA software installed on the appliance.

Onboard multiple ASAs to Security Cloud Control Firewall Management

Security Cloud Control Firewall Management allows you to bulk onboard ASA devices by providing the necessary information for all the ASA devices in a .CSV file.

As the ASA devices are being onboarded, you can use the filter pane to show which onboarding attempts are queued, loading, complete, or have failed.

Before you begin

- Prepare a .CSV file with the connection information for the ASA devices you want to onboard. Add the information about each ASA on a separate line. To include a comment, add a # at the beginning of the line.
  - ASA location (either IP address or FQDN)
  - ASA administrator username
  - ASA administrator password
  - (Optional) Device name for Security Cloud Control Firewall Management
  - (Optional) device labels for Security Cloud Control Firewall Management
  - To add one label, add the label name to the last CSV field.
  - To add more than one label to a device, surround the values with quotation marks. For example, `alpha,beta,gamma`.

- To add a category and choice label, separate the two values with a colon (:). For example, `Rack:50`.

Here is a sample configuration file.

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

Caution Security Cloud Control Firewall Management does not validate any of the data in the .CSV file. You need to ensure the accuracy of the entries.

Follow these steps to onboard multiple ASAs to Security Cloud Control Firewall Management:

Procedure

Step 1 Choose Security Devices.

Step 2 Click the plus button to onboard an ASA.

Step 3 On the Onboarding page, click the **Multiple ASAs** tile.

Step 4 Click **Browse** to locate the .CSV file containing your ASA entries. The devices you specify appear in the ASA Bulk Onboarding table as queued and are ready for onboarding.

Caution
Stay on the ASA Bulk Onboarding page until the onboarding process is complete. If you leave the page, the onboarding process stops.

Step 5 Click **Start**.

The status column in the ASA Bulk Onboarding table shows the progress of onboarding. When onboarding finishes, the status displays "Complete."

To pause bulk onboarding and resume later, refer to Pause and resume onboarding multiple ASA devices, on page 6.

The ASA devices are successfully onboarded to Security Cloud Control Firewall Management and appear with "Complete" status in the ASA Bulk Onboarding table.

Pause and resume onboarding multiple ASA devices

This task allows you to control the bulk onboarding process by pausing it when needed and resuming it later without losing progress on devices that have already been processed.

During bulk onboarding of multiple ASA devices, you may need to temporarily stop the process and resume it later. The system maintains the state of already onboarded devices and continues with the remaining queued devices when resumed.

Procedure

Step 1 To pause the onboarding process, click **Pause**.

Security Cloud Control Firewall Management completes onboarding any device it has started.

Step 2 To resume bulk onboarding, click **Start**.

Security Cloud Control Firewall Management will begin onboarding the next queued device.

The bulk onboarding process can be paused and resumed as needed. If you leave the page after pausing, you must return and restart the process. Security Cloud Control Firewall Management identifies already onboarded devices, flags duplicates from this new attempt, and quickly starts onboarding the remaining queued devices.

Create and import an ASA model to Security Cloud Control Firewall Management

This task allows you to create and import an ASA model to Security Cloud Control Firewall Management, enabling configuration management and offline policy setup for ASA devices.

Use this process when you need to download an ASA device configuration file from the management interface to your local computer for further configuration management tasks.

Procedure

Step 1 Choose Security Devices.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab.

Step 4 Select an ASA device. In the **Management** section, click **Configuration**.

Step 5 To download the device configuration to your local computer, click **Download**.

The ASA device configuration file is downloaded to your local computer and can be used for creating and importing an ASA model with device identity, labels, and offline policy configuration.

Import ASA configuration

Import your Cisco ASA configuration file to enable offline management of ASA security devices through the platform interface.

Use this procedure when you need to onboard ASA security devices for offline management by uploading existing configuration files to the platform.

Before you begin

The ASA running configuration file you are onboarding must be less than 4.5 MB. Confirm the size of the configuration file before you onboard it.

Follow these steps to import ASA configuration:

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose Security Devices.

Step 3 Click the add button () to import the configuration file.

Step 4 Click **Import configuration for offline management**.

Step 5 Select the **Device Type** as **ASA**.

Step 6 Click **Browse**, and select the configuration file in text format to upload.

Step 7 After labeling your model device, you can view it in the **Security Devices** list.

Note
The configuration may take some time to be analyzed, depending on its size and the number of other devices or services.

Configuration import for offline device management

Configuration import for offline device management is a feature that

- allows you to review, analyze, and optimize device settings without requiring access to a live device in your network
- creates models that represent copies of device configurations for policy review, planning, and reuse, and
- processes uploaded configuration files so they appear in the **Security Devices** list for labeling, reviewing, and managing like other supported devices.

Supported device types

You can import the configurations for these device types into Security Cloud Control Firewall Management:

- Adaptive Security Appliance (ASA): You can upload an ASA configuration file to create an ASA model for offline review and management. For more information, refer to Create and Import an ASA Model.
- Cisco IOS devices such as Aggregation Services Routers (ASRs) and Integrated Services Routers (ISRs): You can upload a text-based running configuration file to create an IOS model for offline analysis and reuse.