Configuring ASA Devices

This chapter covers the following sections:

Update ASA Connection Credentials in Security Cloud Control

In the process of onboarding an ASA, you entered the username and password Security Cloud Control must use to connect to the device. If those credentials are changed on the device, use the **Update Credentials** device action to update those credentials on Security Cloud Control as well. This feature allows you to update the credentials on Security Cloud Control without having to re-onboard the device. The username and password combination you switch to must already exist on the ASA or Authentication, Authorization, and Accounting (AAA) server for that user. This process only affects the Security Cloud Control database; no changes to the ASA configuration are made when using the Update Credentials feature.

Procedure

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

Step 2 Click the **Devices** tab and then click **ASA**.

Step 3 Select the ASAs whose connection credentials it is you want to update. You can update the credentials on one or multiple ASAs at once.

Step 4 In the **Device Actions** pane, click **Update Credentials**.

Step 5 Select the Cloud Connector or the Secure Device Connector (SDC) you use to connect the ASA(s) to Security Cloud Control.

Step 6 Enter the new username and password you want to use to connect to the ASAs.

Step 7 After the credentials are changed, Security Cloud Control syncs the device.

Note If Security Cloud Control fails to sync the device, the connectivity status in Security Cloud Control may show "Invalid Credentials." If that's the case, you may have tried to use an invalid username and password combination. Make sure the credentials you want to use are stored on your ASA or AAA server, and try again.

Move an ASA from one SDC to Another

Security Cloud Control supports the use of more than one SDC per tenant. You can move a managed ASA from one SDC to another using this procedure:

Procedure

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

Step 2 Select the ASAs you want to move to the other SDC.

Step 3 In the Device Actions pane, click **Update Credentials**.

Step 4 Click the Secure Device Connector button and select the SDC you want to move the device to.

Step 5 Enter the administrator username and password you used to onboard the ASA, and click Update. You do not have to deploy these changes to the device.

ASA Interface Configuration

Security Cloud Control simplifies ASA interface configuration by providing a user-friendly interface that eliminates the need to use the command line interface. You have complete control over configuring the ASA's physical interfaces, subinterfaces, and EtherChannels. Moreover, you can also view Virtual Tunnel Interfaces that are created during route-based site-to-site VPN, but they are read-only. You can use Security Cloud Control to configure and edit data interfaces or the management/diagnostic interface on an ASA device.

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for traffic to pass through it. If the interface is a member of a bridge group, naming the interface is sufficient. If the interface is a bridge virtual interface (BVI), you need to assign the BVI an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs.

The interface list shows the available interfaces, their names, addresses, and states. You can change the state of an interface, on or off, or edit an interface, by selecting the interface row and clicking **Edit** in the Actions pane. The list shows the interface characteristics based on your configuration. Expand an interface row to see subinterfaces or bridge group member.

Management Interface

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management Slot/Port interface (if available for your model)

Use MTU Settings

The MTU specifies the maximum frame payload size that the device can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, VLAN tagging, or other overhead. For example,

when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Read-only Support for Virtual Tunnel Interface (VTI)

Configuring a route based site-to-site VPN tunnel between two ASA devices creates a Virtual Tunnel Interface (VTI) between the devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control, which discovers and lists them on the **ASA Interfaces** page but doesn't support their management.

Configure an ASA Physical Interface

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 Click a physical interface that you want to configure, and click **Edit**.

The **Editing Physical Interface** dialog box appears.

Step 5 In the **Logical Name** field, enter a name for the interface.

Step 6 Continue with one of the following procedures:

- Configure IPv4 Addressing for ASA Physical Interface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Physical Interface, on page 5 if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the ASA Physical Interface.

Configure IPv4 Addressing for ASA Physical Interface

Procedure

Step 1 In the **Edit Physical Interface** dialog box, configure the following in the **IPv4 Address** tab:

- **Type**: You can use either static IP addressing or DHCP for the interface.

  Static - Choose this option if you want to assign an address that should not change.

  - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.

- **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

  For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

Step 2 Click **Save** if you are done or continue with one of these procedures.

- Configure IPv6 Addressing for ASA Physical Interface, on page 5 if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the ASA Physical Interface.

Configure IPv6 Addressing for ASA Physical Interface

Procedure

Step 1 In the **Editing Physical Interface** dialog box, click the **IPv6 Address** tab.

Step 2 Configure the following:

- **State**: To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

  Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

- **Address Auto Configuration**:

  Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

  Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Suppress RA**: Check this box if you want to suppress router advertisements. The device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

  You might want to suppress these messages on any interface for which you do not want the device to supply the IPv6 prefix (for example, the outside interface).

- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **Link-Local Address**: If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

  Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby Link-Local Address**: Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other device, to which this interface is connected.

- **Static Address/Prefix**: If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. You can add another static address.

- **Standby IP Address**: If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 3 Click **Save** if you are done or continue with one of these procedures.

- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the ASA Physical Interface.

Configure Advanced ASA Physical Interface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Procedure

Step 1 In the **Editing Physical Interface** dialog box, click the **Advanced** tab.

Step 2 Configure the following advanced settings:

- **HA Monitoring**: Enable to include the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
- **Management Only**: Enable to make a data interface management only.

  A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **Duplex and Speed (Mbps)**: The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. The options listed are only those supported by the interface. Before setting these options for interfaces on a network module, please read Limitations for Interface Configuration.
  - **Duplex**: Choose Auto, Half, or Full. Auto is the default when the interface supports it.
  - **Speed**: Choose Auto to have the interface negotiate the speed (this is the default), or pick a specific speed: 10, 100, 1000, 10000 Mbps. You can also select these special options:
- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.
- **MAC Address**: The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**: For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 3 If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the ASA Physical Interface.

Step 4 Click **Save**.

Enable the ASA Physical Interface

Procedure

Step 1 Select the physical interface you want to enable.

Step 2 Move the **State** slider at the top right of the window associated with the interface's logical name.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made.

Add an ASA VLAN Subinterface

VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.

- Configure ASA VLAN Subinterfaces

  Configure IPv4 Addressing for ASA Subinterface, on page 9
- Configure IPv6 Addressing for ASA Subinterface, on page 10
- Configure Advanced ASA Subinterface Options, on page 11
- Enable the Subinterface, on page 12

Configure ASA VLAN Subinterfaces

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 You can add a subinterface using one of the following methods:

- Choose  > **Subinterface**
- Click a physical interface that you want to configure and in the **Actions** pane on the right, click **New Subinterface**.

Step 5 In the **VLAN ID** field, enter the VLAN ID between 1 and 4094.

Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.

Step 6 In the **Subinterface ID** field, enter the subinterface ID as an integer between 1 and 4294967293.

The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.

Step 7 Continue with one of the following procedures:

- Configure IPv4 Addressing for ASA Subinterface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Subinterface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Subinterface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure IPv4 Addressing for ASA Subinterface

Procedure

Step 1 In the **Creating Subinterface** dialog box, configure the following in the **IPv4 Address** tab:

- **Type**: You can use either static IP addressing or DHCP for the interface.

  Static - Choose this option if you want to assign an address that should not change.

  - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
  - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

    For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

  DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

  You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

Step 2 Click **Save** if you are done or continue with one of these procedures.

- Configure IPv6 Addressing for ASA Subinterface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Subinterface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the ASA Physical Interface.

Configure IPv6 Addressing for ASA Subinterface

Procedure

Step 1 In the **Creating Subinterface** dialog box, click the **IPv6 Address** tab.

Step 2 Configure the following:

- **State**: To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

  Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

- **Address Auto Configuration**:

  Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

  Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Suppress RA**: Check this box if you want to suppress router advertisements. The device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

  You might want to suppress these messages on any interface for which you do not want the device to supply the IPv6 prefix (for example, the outside interface).

- **DAD Attempts** How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **Link-Local Address**: If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

  Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby Link-Local Address**: Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other device, to which this interface is connected.
- **Static Address/Prefix**: If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. You can add another static address.
- **Standby IP Address**: If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 3 Click **Save** if you are done or continue with one of these procedures.

- Configure Advanced ASA Subinterface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure Advanced ASA Subinterface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Procedure

Step 1 In the **Creating Subinterface** dialog box, click the **Advanced** tab.

Step 2 Configure the following advanced settings:

- **HA Monitoring**: Enable to include the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
- **Management Only**: Enable to make a data interface management only.

  A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is

not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **MAC Address**: The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**: For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 3 If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Subinterface.

Step 4 Click **Save**.

Enable the Subinterface

Procedure

Step 1 Select the subinterface you want to enable.

Step 2 Move the **State** slider at the top right of the window associated with the interface's logical name.

Step 3 Review and deploy the changes you made.

Remove ASA Subinterface

Use the following procedure to remove an subinterface from ASA.

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 On the **Interfaces** page, expand the physical interface linked with the subinterface you want to delete and then select that specific subinterface.

Step 5 In the **Actions** pane located to the right, click **Remove**.

Step 6 Confirm you want to delete the EtherChannel interface and click **Delete**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made.

About ASA EtherChannel Interfaces

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

See the **EtherChannel and Redundant Interfaces** chapter of ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X, Y for more information on ASA EtherChannel interfaces.

Configure ASA EtherChannel

Use this procedure to add a new EtherChannel interface to an ASA.

Before you begin

To configure EtherChannel on ASA interface, the following prerequisites must be met:

- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, except for the Secure Firewall 3100, which supports different interface capacities as long as the speed is set to Detect SFP; in this case, the lowest common speed is used.
- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name.
- You cannot add an interface part of another EtherChannel interface group, Switchport interfaces, and interfaces with subinterfaces.

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 Choose  > **EtherChannel Interface**.

Step 5 In the **Logical Name** field, provide a name for the EtherChannel interface.

Step 6 In the **EtherChannel ID**, enter an integer between 1 and 8.

Step 7 Click the drop-down button for **Link Aggregation Control Protocol** and select one of the two options:

- **Active** —Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **On**— The EtherChannel is always on, and LACP is not used. An **on** EtherChannel can only establish a connection with another EtherChannel that is also configured to be **on**.

Step 8 Search for and select the interfaces you want to include in the EtherChannel as members. You **must** include at least one interface.

Warning If you add an EtherChannel interface as a member and it already has an IP address configured, Security Cloud Control removes the IP address of the member.

Step 9 Select the **IPv4**, **IPv6**, or **Advanced** tab to configure the IP address of the subinterface.

- Configure IPv4 Addressing for ASA Physical Interface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Physical Interface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 10 Move the **State** slider at the top right of the window to enable the EtherChannel interface.

Step 11 Click **Save**.

Step 12 Preview and Deploy Configuration Changes for All Devices the changes you made.

Edit ASA EtherChannel

Use this procedure to edit an existing EtherChannel on ASA.

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 4 On the **Interfaces** page, select the EtherChannel interface you want to edit.

Step 5 In the **Actions** pane located to the right, click **Edit**.

Step 6 Modify the values you want and click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made.

Remove ASA EtherChannel Interface

Use the following procedure to remove an EtherChannel interface from ASA.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **ASA** tab.
Step 3 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
Step 4 On the **Interfaces** page, select the EtherChannel interface you want to delete.
Step 5 In the **Actions** pane located to the right, click **Remove**.
Step 6 Confirm you want to delete the EtherChannel interface and click **Delete**.
Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made.

ASA System Settings Policy in Security Cloud Control

Introduction to ASA System Settings Policy

Manage your ASA device's operations and functionalities using a System Settings policy. This policy includes essential configurations like domain name services, enabling the secure copy server, message logging, and permitting VPN traffic without checking ACLs. By setting up a policy, you can ensure that your device is properly configured to maintain a secure network environment.

When configuring an ASA device, it's important to note that you have the option to manage multiple devices' settings with a shared system settings policy, or you can individually edit the settings for any single device.

Shared System Settings Policy

A shared system settings policy applies to multiple ASA devices in your network. It makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes made to a parameter of a shared policy affect the other ASA devices that use the policy.

Choose **Policies** > **ASA** > **System Settings**. See Create an ASA Shared System Settings Policy, on page 15.

You can also modify the device-specific system settings specific to a single ASA device to override the shared system settings policy values. Choose **Security Devices** > **ASA device** > **Management** > **Settings**. See Configure or Modify Device Specific System Settings, on page 22.

Create an ASA Shared System Settings Policy

Use this section to create a new shared system settings policy for ASA devices.

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 2 Click  .

Step 3 In the **Name** field, enter a name for the policy and click **Save**.

Step 4 In the edit ASA shared system settings page, configure the parameters you want:

- Configure Basic DNS Settings, on page 16
- Configure HTTP Settings, on page 17
- Set the Date and Time Using an NTP Server, on page 18
- Configure SSH Access, on page 19
- Configure System Logging, on page 19
- Enable Sysopt Settings, on page 21

Note

- An orange dot () on the corresponding parameter highlights unsaved changes.
- The denied symbol () highlights parameters that use existing local values from the device.

Configure Basic DNS Settings

You need to configure a DNS server so that the ASA can resolve host names to IP addresses. You also must configure a DNS server to use fully qualified domain names (FQDN) network objects in access rules.

Procedure

Step 1 In the edit ASA system settings page, click **DNS** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 In the **DNS** section, click  to configure servers.

- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify DNS server's IP address.
- **Interface Name**: Specify the interface where the DNS lookup should be enabled.

Note Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

Step 4 Click **Save**.

Step 5 In the **Domain name** field, specify the domain name for the ASA.

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com" and specify a syslog server by the unqualified name of "jupiter," then the ASA qualifies the name to "jupiter.example.com."

Step 6 In the **DNS Lookup** section, click + and specify the interface name.

If you do not enable DNS lookup on an interface, then the ASA will not communicate with the DNS server on that interface. Make sure to enable DNS lookup on all interfaces that will be used to access DNS servers.

Note To remove a configured interface, you can click the delete icon under **Actions**.

Step 7 Click **Save**.

Configure HTTP Settings

To access the ASA interface for management access, you must specify the addresses of all hosts/networks which are allowed to access the ASA using HTTP. If you configure HTTP redirect to redirect HTTP connections to HTTPS automatically, you must enable an access rule to allow HTTP; otherwise, the interface cannot listen to the HTTP port.

Procedure

Step 1 In the edit ASA system settings page, click **HTTP** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Check the **Enable HTTP Server** check box to enable the HTTP server.

Step 4 In the **Port Number** field, set the port number. The port identifies the port from which the interface redirects HTTP connections.

Warning If you change the HTTP port on your device, it may cause some problems with its connection to Security Cloud Control. It's important to remember this if you plan to alter any settings related to your device's network connection.

Step 5 Click + to add HTTP information.

- **Interface**: Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using HTTP.
- **Netmask**: Specify the subnet mask for the network.

Note To remove a host, you can click the delete icon under **Actions**.

Step 6 Click **Save**.

Set the Date and Time Using an NTP Server

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is.

Time derived from an NTP server overrides any time set manually.

The ASA supports NTPv4.

Procedure

Step 1 In the edit ASA system settings page, click **NTP** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Click  to add NTP server details.

- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the NTP server's IP address.

  You cannot enter a hostname for the server; the ASA does not support DNS lookup for the NTP server.
- **Key Id**: Enter a number between 1 and 4294967295.

  This setting specifies the key ID for this authentication key, which enables you to use authentication to communicate with the NTP server. The NTP server packets must also use this key ID.
- **Interface Name**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

  NTP uses an algorithm to determine which server is the most accurate and synchronizes to it. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one.
- **Prefer**: (optional) Check the **Preferred** check box to set this server as a preferred server.

Note To remove an NTP server, you can click the delete icon under **Actions**.

Step 4 Click **Save**.

Configure SSH Access

You can enable the secure copy (SCP) server on the ASA. Only clients that are allowed to access the ASA using SSH can establish a secure copy connection.

Procedure

Step 1 In the edit ASA settings policy page, click **SSH** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Enable **Enable Scopy SSH** (secure copy SSH).

Step 4 In the **Timeout in Minutes** field, set the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases, and should be increased until all pre-production testing and troubleshooting have been completed.

Step 5 Click  and configure the following:

- **Interface**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using SSH.
- **Netmask**: Specify the subnet mask for the network.

Note To remove SSH details, you can click the delete icon under **Actions**.

Step 6 Click **Save**.

Configure System Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

Security Levels

The following table lists the syslog message severity levels.

Table 1: Syslog Message Severity Levels

Level Number	Security Level	Description
0	**emergencies**	System is unusable

Level Number	Security Level	Description
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only. Log at this level only temporarily, when debugging issues. This log level can potentially generate so many messages that system performance can be affected.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

Procedure

Step 1 In the edit ASA system settings page, click **Syslog** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Configure the following:

- **Logging Enabled**: Enable secure logging.
- **Timestamp Enabled**: Enable to include the date and time in syslog messages.
- **Permit host down**: (Optional) Disable the feature to block new connections when a TCP-connected syslog server is down.
- **Buffer Size**: Specify the size of the internal log buffer. The allowed range is 4096 to 1048576 bytes.
- **Buffered Logging Level**: Specify which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location.
- **Console Logging Level**: Specify which syslog messages should be sent to the console port.
- **Trap Logging Level**: Specify which syslog messages should be sent to the syslog server.

Step 4 Click  to add Syslog server details.

- **Interface Name**: Specify the interface name on which the syslog server resides. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the IP address of the syslog server.
- **Protocol**: Choose the protocol (**TCP** or **UDP**) the ASA should use to send syslog messages to the syslog server.
  - **Port**: Specify the port that the syslog server listens to for syslog messages. The allowed TCP port range is 1 to 65535, and the UDP port range is 1025 to 65535.
  - **Log messages in Cisco EMBLEM format (UDP only)**: Enables EMBLEM format logging for the syslog server with UDP only.
  - **Enable secure syslog using SSL?**: Specifies that the connection to the remote logging host should use SSL/TLS for TCP only.
- **Reference Identity**: Specify the reference identity type to enable RFC 6125 reference identity checks on the certificate based on the previously configured reference identity object. See Configure Reference Identities for details on the reference identity object.

Note To remove a Syslog server, you can click the delete icon under **Actions**.

Step 5 Click **Save**.

Enable Sysopt Settings

The crypto map ACL bound to the outgoing interface either permits or denies IPsec packets through the VPN tunnel. IPsec authenticates and deciphers packets that arrive from an IPsec tunnel, and subjects them to evaluation against the ACL associated with the tunnel.

ACLs define which IP traffic to protect. For example, you can create ACLs to protect all IP traffic between two subnets or two hosts.

Procedure

Step 1 In the edit ASA system settings page, click **Sysopt** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Enable **Allow VPN traffic to bypass interface access lists** bypasses the ACL inspection.

Step 4 Click **Save**.

Assign a Policy from the Shared System Settings Page

After configuring a shared system settings policy, assign onboarded ASA devices and deploy the settings to the devices for the changes to take effect. Any change made to the policy affects the devices that are associated with the policy.

You can also Assign a Policy from Device-Specific Settings Page page.

Note You can associate an ASA device to only one shared system settings policy.

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 2 Select a shared policy and click **Edit**.

Step 3 Click the filter appearing beside the policy name to assign devices.

Step 4 Select the ASA devices you want to associate with the selected policy and click **OK**.

Note The checkboxes are ticked for devices that are already associated with the selected policy.

If you see a red icon  , it means that an error has occurred while applying the shared system settings policy to your devices. To troubleshoot the issue, click the policy on the **ASA System Settings** page and in the **Error Detected** pane, click the **Device Workflows** to get more information.

Step 5 Deploy Configuration Changes Made Using the Security Cloud Control GUI the changes you have made.

Configure or Modify Device Specific System Settings

A device-specific system settings are existing values specific to an ASA device that can be modified using Security Cloud Control. You can override the shared system settings policy values with existing device-specific values for parameters you want.

This topic describes configuring an onboarded ASA device's system settings.

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

You will see the device-specific system settings of the selected ASA device.

Note If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. You can also assign a policy from the device-specific settings page. Select the ASA devices you want to associate with the selected policy and click **OK**

Step 4 Configure or modify the values of the system settings you want and click **Save**.

Note The field descriptions for a shared and device-specific system settings remain the same. You can click the corresponding link below for more information.

- Configure Basic DNS Settings, on page 16
- Configure HTTP Settings, on page 17
- Set the Date and Time Using an NTP Server, on page 18
- Configure SSH Access, on page 19
- Configure System Logging, on page 19
- Enable Sysopt Settings, on page 21

You can click **Return to Security Devices** to navigate to the **Security Devices** page.

Step 5 Click **Save** after making the changes.

Note An orange dot () on the corresponding parameter highlights unsaved changes.

Assign a Policy from Device-Specific Settings Page

You can also assign a policy from the device-specific settings page of an onboarded ASA device.

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

You will see the device-specific settings of the selected ASA device.

Note If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. Select the ASA devices you want to associate with the selected policy and click **OK**

Step 4 Click the **Parent Policy** button to assign a shared system settings policy.

Step 5 Select a policy and click **Apply**.

Step 6 Deploy Configuration Changes Made Using the Security Cloud Control GUI the changes you have made.

Auto Assignment of ASA Devices to a Shared System Settings Policy

When onboarding a new ASA device, or checking for changes or handing out-of-band changes for existing devices, Security Cloud Control verifies whether:

- The device-specific settings match a pre-existing shared system settings policy. If there is a match, the device gets assigned to the shared system settings policy.
- The device-specific settings of the onboarded devices match each other. If they do, a new shared system settings policy gets created automatically, and devices with the same local settings are assigned to this shared policy.

Note You can rename the Shared Settings policy whether it was created by the user or the system.

Filter ASA Shared System Settings Policy

If you're searching for specific shared system settings policies on the ASA System Setting page, you can use filters based on issues and usage to narrow down your search and find what you're looking for more easily.

Click **Policies** > **ASA** > **System Settings** >  .

- **Issues**:
  - **Issue Detected**: Displays only the policies that have issues when applying devices to them.
  - **No issue**: Displays only the policies that are successfully applied to devices.
- **Usage**:
  - **In Use**: Displays policies that have are assigned to devices.
  - **Unused**: Displays policies that have not been assigned to any devices yet.

Disassociate Devices from Shared System Settings Policy

If an ASA device is no longer needed in the shared system settings policy, you can easily dissociate it. The device detaches from the policy when:

- Changes are made to the device-specific settings, where the corresponding setting on the shared policy is not configured to retain existing values from the device.
- Devices are detached manually from the shared system settings policy.
- Shared system settings policy is deleted from Security Cloud Control. However, this doesn't delete the device. See Delete Shared Settings Policy, on page 25.

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 2 Select a shared policy and click **Edit**.

Step 3 Click the filter appearing beside the policy name to detach devices.

Step 4 Uncheck the devices you want to detach from the selected shared system settings policy and click **OK**.

Note The changes are saved automatically and don't require any manual deployment.

Delete Shared Settings Policy

If you want to remove some shared settings policies, you have the option to select one or more of them and delete them. However, it's important to note that you can only delete them if they haven't been applied or committed to any devices yet.

Before you begin

Ensure the devices are dissociated from the shared settings policy you wish to delete. See Disassociate Devices from Shared System Settings Policy for more information.

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 2 Select a shared policy and click **Delete**.

Step 3 Click **OK** to confirm your action.

Note If you delete an ASA from Security Cloud Control, the device-specific settings and configurations will also be deleted, and the device references will be removed from the shared settings policy.

ASA Routing in Security Cloud Control

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which include route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with various information. Destination or next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables can also include other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of various messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message that is sent between routers, informs other routers of the state of the sender links. Link information can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

About ASA Static Route

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

For general information on how ASA routing concepts and CLI commands, see the following documents:

- *Static and Default Routes* chapter from ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X,Y.
- *Static and Default Routes* chapter from CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, X,Y.

Default Route

The simplest option is to configure a default static route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the ASA sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

You should always define a default route.

Static Route

You might want to use static routes in the following cases:

- Your networks use an unsupported router discovery protocol.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the ASA.
- You are using a feature that does not support dynamic routing protocols.

Static Route Tracking

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The ASA implements static route tracking by associating a static route with a monitoring target host on the destination network that the ASA monitors using ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address.
- The next hop gateway address (if you are concerned about the availability of the gateway).
- A server on the target network, such as a syslog server, that the ASA needs to communicate with.
- A persistent network object on the destination network.

Configure ASA Static Route

A static route defines where to send traffic for specific destination networks.

This section describes the steps to add a static route to an ASA device.

Procedure

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

Step 2 Click the **ASA** tab.

Step 3 Select a device you want to configure a static route.

Step 4 In the **Management** pane on the right, click **Routing**.

Step 5 Click  to add a static route.

Step 6 You can enter a **Description** for the route.

Step 7 Select whether the route is for an **IPv4** or **IPv6** address.

Step 8 Configure the route properties:

- **Interface**: Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.

  You can use a **Null0** route to forward unwanted or undesirable traffic so the traffic is dropped. Static Null0 routes have a favorable performance profile. You can also use static null0 routes to prevent routing loops.

  The ASA CLI accepts both Null0 or null0 strings.
- **Gateway IP**: (Not applicable to a **Null0** route) Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.
- **Metric**: The administrative distance for the route, between 1 and 254. The default for static routes is 1. If there are additional routers between the interface and the gateway, enter the number of hops as the administrative distance.

  Administrative distance is a parameter used to compare routes. The lower the number, the higher precedence the route is given. Connected routes (networks directly connected to an interface on the device) always take precedence over static routes.
- **Destination IP**: Select the network object(s), that identifies the destination network, that contains the host(s), that uses the gateway in this route.
- **Destination Mask** (only for IPv4 addressing): Enter the subnet mask for the destination IP.
- **Tracking** (only for IPv4 addressing): Enter a unique identifier for the route tracking process.

Step 9 Click **Save**.

Step 10 Deploy Configuration Changes Made Using the Security Cloud Control GUI the changes you made, or wait and deploy multiple changes at once.

Edit ASA Static Route

You can edit the static route parameters associated with an ASA device.

Note However, you cannot select a different IP version while modifying the static route. Alternatively, you can create a new static route based on your requirement.

Procedure

Step 1 Select an ASA device you want to edit the static route.

Step 2 In the **Management** pane on the right, click **Routing**.

Step 3 In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Edit**.

Step 4 Modify the values you want and click **Save**. See Configure ASA Static Route, on page 27 for information on the routing parameters.

Step 5 Deploy Configuration Changes Made Using the Security Cloud Control GUI the changes you made, or wait and deploy multiple changes at once.

Delete a Static Route

Before you begin

Deleting a static route may impact the connectivity to your device's local SDC or Security Cloud Control. Ensure a proper disaster recovery procedure is in place for any connectivity loss.

Procedure

Step 1 Select an ASA device you want to delete.

Step 2 In the **Management** pane on the right, click **Routing**.

Step 3 In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Delete**.

Step 4 Click OK to confirm the changes.

Step 5 Deploy Configuration Changes Made Using the Security Cloud Control GUI the changes you made, or wait and deploy multiple changes at once.

Manage Security Policies in Security Cloud Control

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use Security Cloud Control to configure security policies on many different types of devices.

- Create an ASA Access List
- Network Address Translation, on page 44

Manage ASA Network Security Policy

The ASA network security policy includes access control lists (ACLs) that determine whether to permit or deny traffic from accessing another network through the ASA firewall. This section outlines the steps to create an ASA access list and configure access rules within it. It also details the steps to assign an interface to an access control list and share it among other ASA devices managed by Security Cloud Control.

About ASA Access Control Lists and Access Groups

ASA Access Control Lists

Access control lists (ACLs) are used to identify traffic flows based on various characteristics such as source and destination IP address, IP protocol, ports, source, and other parameters.

The following is an access list sample:

```
access-list ACL extended permit ip any any
```

`ACL` is the name of the access list.

You can avoid the creation of the same access list on multiple devices individually, and instead create a single access list and share it across multiple ASA devices. Changes made to the shared access list automatically apply to all the devices to which the ACL is assigned. You also have the option to copy the access list to other ASA devices as needed.

Access Rules

An access list includes access rules that permit or deny traffic flow to a network based on specific characteristics such as source and destination IP addresses, IP protocol, port number, and security group tags.

ASA Access Groups

An access group is a specific association that is established when an access list is assigned to a device interface configured for traffic flow in any direction. The access list contains specific rules that either permit or deny traffic passing through the device interface.

The following is an access group sample that is created when a device interface is assigned to an access list.

```
access-group ACL out interface giginterface0
```

`ACL` is the name of the access list and `giginterface0` is the logical name of the device interface that is assigned to the access list.

Note To use API endpoints to manage your ASA access groups, see Get Access Groups on the Cisco DevNet website.

Create an ASA Access List

When configuring an access list on an ASA firewall, a rule is automatically created to allow traffic from a source to a destination outside your network. You can create additional rules and assign the access list to an interface to regulate the traffic network.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 Click **Create Access List**.

Step 5 In the **Name** field, enter a name for the access list and click **Save**.

Note You cannot have two access lists with the same name on a device.

Step 6 Click **Save**.

Security Cloud Control creates an access group and a default rule that permits all traffic.

You can now add new rules to the access list. See Add a Rule to an ASA Access List, on page 30.

What to do next

- To add new rules to the access list, see Add a Rule to an ASA Access List, on page 30.
- To assign interfaces and traffic directions to the access list, see Assign Interfaces to ASA Access Control List, on page 33.

Add a Rule to an ASA Access List

You can add rules in ascending order by rule number. Packets will be verified against the rules in the sequence in which the rules were created, with the first rule taking precedence, followed by subsequent rules. You can adjust the position of any rule, if required.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, select an access list that you want.

Step 5 Click the **Add Rule** ( ) icon that is displayed on the right.

Note In the ordered list, hover over the desired position and click **Add Rule Here**.

Step 6 In the **New Access Rule** window, provide the following information:

- **Order**: Select where you want to insert the rule in the ordered list of rules. Rules are applied on a first-match basis and prioritized by position in the list of rules from 1 to last.
- **Action**: Specify whether you are allowing (permitting) the described traffic or are blocking (dropping) it.
- **Protocol**: Specify the protocol of the traffic, such as IP, TCP, UDP, ICMP, or ICMPv6. The default is IP, but you can select a more specific protocol to target traffic with more granularity.
- **Source/Destination**: Define the source (originating address) and destination (target address of the traffic flow). You typically configure the IPv4 address of hosts or subnets, which you can represent with network object groups. You can assign only one object to the source or destination. To create a new network object or group, see Create or Edit ASA Network Objects and Network Groups.
- **Port**: Select the port object that pairs a service type, such as TCP or UDP, and a port number or a range of port numbers.
- **SGT Group**: Assign the security group you want from the list. By default, the value is **Any**. See About Security Group Tags in ASA Policies.
- **Time Range**: Define a time range for ASA network policies to allow access to networks and resources based on time of day. See ASA Time Range Objects.
- **Logging**: Activity resulting from a network policy rule is not logged by default. You can activate logging for individual rules. See About System Log Activity .

Step 7 Click **Save**.

The rule is added to the access list and set to **Active** state.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

About System Log Activity

When you set up a new rule, you can specify how often and at what severity level you want to collect its activity. To do this, you can select the corresponding severity levels and then choose the frequency of data collection. This will ensure that you have the necessary information to monitor and analyze the activity generated by your rules.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

You have the option to adjust the logging interval, which indicates how frequently the log records are updated. This interval is measured in seconds and can be set from 1 to 600. By default, the interval is set to 300 seconds.

This interval value is also utilized as a timeout period for removing an inactive flow from the cache that collects drop statistics.

Table 2: Log Rule Activity

Security Level	Description
emergencies	System is unusable.
alert	Immediate action is needed.
critical	Critical conditions.
error	Error conditions.
warning	Warning conditions.
notification	Normal but significant conditions.
informational	Informational messages only.
debugging	Debugging messages only.

Deactivate Rules in an Access Control List

When you create a new rule in an access control list, it is activated by default. However, you can temporarily deactivate individual rules to optimize traffic flow, resolve conflicts, or isolate issues.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose the access control list you want.

Step 5 In the rule list, check the corresponding rule check box that you want.

Step 6 In the selected row, slide the **Active** setting off.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

About Security Group Tags in ASA Policies

If you onboard an ASA that uses security group tags (SGT) in its access control rules, Security Cloud Control allows you to edit the rules that use SGT groups and manage the policies that have these rules. However, you cannot create SGT groups or edit them using the Security Cloud Control GUI. To create or edit SGT groups, you must use ASA's Adaptive Security Device Manager (ASDM) or the CLI available in Security Cloud Control.

In Security Cloud Control's object page, when looking at the details of SGT groups, you'll see that those objects are identified as noneditable, system-provided objects.

Security Cloud Control administrators can perform these tasks on ACLs and ASA policies that contain SGT groups:

- Edit all aspects of ACLs except the source and destination security groups.
- Copy a policy containing SGT groups from one ASA to another.

For detailed instruction, on configuring Cisco TrustSec using the command line interface, see the "ASA and Cisco TrustSec" chapter of the ASA CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide pertaining to your ASA release.

Assign Interfaces to ASA Access Control List

When you assign ASA interfaces to access control list, the device establishes a specific association between the list and interfaces. The rules that are associated with access control list are applied only to the interfaces through which the traffic flows in the specified directions.

You can only assign one access list per interface for a single traffic flow direction.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane displayed on the right, click **Assign Interfaces**.

Step 6 From the **Interface** drop-down list, choose an interface.

Step 7 From the **Direction** drop-down list, specify the direction for applying the selected access list.

The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

To apply the access list to all the interfaces on the ASA device, see Create an ASA Global Access List, on page 33.

Step 8 Click **Save**.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Create an ASA Global Access List

Global access policies are network policies that are applied to all the interfaces on an ASA. These policies are only applied to inbound network traffic. You can create a global access policy to ensure that a set of rules is applied uniformly to all the interfaces on an ASA.

Only one global access policy can be configured on an ASA. However, a global access policy can have more than one rule assigned to it, just like any other policy.

This is the order of rule-processing on the ASA:

1. Interface access rules
2. Bridge Virtual Interface (BVI) access rules
3. Global access rules
4. Implicit deny rules

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.
Step 3 In the **Management** pane on the right, click **Policy**.
Step 4 From the **Selected Access List** drop-down list, choose an access list.
Step 5 In the **Actions** pane displayed on the right, click **Assign Interfaces**.
Step 6 Check the **Create as a global access list** check box.
Step 7 Click **Save**.
Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Share an ASA Access Control List with Multiple ASA Devices

Sharing access policies in network security effectively improves efficiency, consistency, and centralized management, leading to an overall improved security posture. With a shared access control list, you can define access rules once on an ASA device and apply them to other Security Cloud Control-managed ASA devices rather than configuring them separately. This ensures consistency in the network and reduces the risk of misconfigurations. Additionally, shared access control lists provide scalability because networks grow and evolve by allowing you to manage access control lists for increasing users and ASA devices.

Keep the following points in mind:

- Access control list rules are shared, but the interfaces are not included.
- Sharing an access control list with other ASA devices will overwrite any existing access control lists with the same name.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.
Step 3 In the **Management** pane on the right, click **Policy**.
Step 4 From the **Selected Access List** drop-down list, choose an access control list.
Step 5 In the **Actions** pane that is displayed on the right, click **Share**.
Step 6 Select the ASA devices by checking the corresponding check box and click **Save**.

In the **Device Relationships** pane displayed on the right, the ASA devices that share the selected access control list are displayed.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Copy an ASA Access Control List to Another ASA

An ASA access control list can be easily copied to another Security Cloud Control-managed device in the same tenant. After copying an access list file to a target ASA device, any further changes made to the access list won't be automatically applied to the target device. This is different from access control list sharing feature, where changes are automatically applied.

Keep the following points in mind:

- You cannot copy an access list to a target device if that device already has another access list with the same name.
- You cannot copy an access list if another access list on the target device is associated with the same interface and direction.
- You cannot only copy an access list to a disabled interface on the target device.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane on the right, click **Copy**.

Step 6 Select the target device to which you want to copy the access list.

Step 7 Choose an interface and specify the direction for applying the selected access list.

The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

To apply the access list to all the interfaces on the selected target, see Create an ASA Global Access List, on page 33.

Step 8 Click **Copy**.

A message appears at the bottom right corner on the Security Cloud Control screen on a successful copy.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Copy a Rule Within or Across ASA Access Lists and Devices

You can copy an access control rule in the following ways:

- Within the same access list.
- From one access list to another, either within the same ASA device or across different ASA devices.

Note The paste operation fails if you attempt to add a rule that already exists in the access list.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, select an access list that you want.

Step 5 Select a rule by clicking the corresponding check box and in the **Actions** pane on the right, click **Copy**.

Step 6 Perform the following:

- To paste the rule within the same access list, hover the mouse pointer in the desired position until you see the **Paste Rule Here** option and click it. The Add/Edit rule dialog box is displayed, allowing you to modify the copied rule, as identical rules are not permitted in the same access list.
- To paste the rule within the same ASA device, from the **Selected Access List** drop-down list, select an access list you want.
- To paste the rule to a different ASA device, in the left pane, go to **Security Devices** > select an ASA device > **Policy** > **Selected Access List**.

Step 7 To paste the copied rule in the desired position, select a rule that comes after where you want the new rule to be. In the **Actions** pane on the right, click **Paste**. The copied rule will be inserted before the selected rule.

You can use the **Move Up** and **Move Down** buttons to position the rule as needed.

Note Alternatively, you can hover over a desired position in the rule listing table until you see **Paste Rule Here**, and then click it.

Unshare a Shared ASA Access Control List

If the rules governing the interface handling your network become outdated, you can unshare the access control list from the devices currently linked. Unsharing an ASA device from the shared access control list will not have any impact on other ASA devices currently sharing this list.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list.

Step 5 In the **Actions** pane on the right, click **Share**.

Step 6 Uncheck the ASA devices that share the selected access list and click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

View ASA Access Policies Listing Page

Note This view applies to ASA devices that have been migrated to the new policy view. For devices that remain onboarded in the legacy policy view, you will continue to see the old view.

The ASA access policy listing page shows a comprehensive overview of all access lists associated with the ASA devices that have been onboarded to the Security Cloud Control tenant.

Note Click the filter ( ) button, then click **Filter by Device** to search for policies that are either shared across multiple ASA devices or specific to a single ASA device.

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **Access Policies**.

The page provides the following information:

- **Name**: The name of the access list.
- **Device**: The corresponding ASA devices associated with each access list. Additionally, for access lists that are shared across multiple devices, it displays a list of all ASA devices that use the shared access list.

  Click the button to view the ASA devices associated with the selected access list.

  To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

  To return to this page, click **ASA Access Policies**.
- **Interfaces**: The network interfaces to which each access list is assigned.

Step 2 To view the ASA devices associated with an access list, click the corresponding button in the **Device** column.

Step 3 To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

Step 4 To return to the policy listing page, in the top-left corner, click ← **ASA Access Policies**.

Global Search of ASA Access Lists

Use the global search functionality to search the following in your Security Cloud Control tenant:

- ASA devices and all their associated access lists.
- Access lists or shared access lists and their occurrences across all onboarded ASA devices.

Rename an ASA Access Control List

It is possible to modify the name of an access list to suit your specific needs. Whether you want to rename a global access list or a shared access control list, it is a straightforward process. If the access list is shared, changing its name updates the name on all the other devices where the shared access control list is used. Remember that the updated name will only reflect after the configuration is deployed to those devices.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list that you want to rename.

Step 5 Click the **Rename** ( ) icon in the right pane.

Step 6 Click the **Save** ( ) button.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes.

Delete a Rule from an ASA Access Control List

You can remove access rules from the access list, but at least one rule must remain for the list to exist.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 Click an access list and select the rules to be deleted.

Step 5 In the **Actions pane** on the right, click **Remove**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Delete an ASA Access Control List

This procedure can be used to delete the access control list, shared access list, or a global access list. Deleting a shared access list from one device does not impact other devices where the access list is in use. On those devices, the access list persists as a local access list.

Procedure

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

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane displayed on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, choose an access list you want to delete.

Step 5 In the **Actions** pane on the right, click **Delete**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Compare ASA Network Policies

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **Access Policies**.

Step 2 Click **Compare** in the top right corner of the viewer.

Step 3 Select up to two policies to compare.

Step 4 Click **View Comparison** at the bottom of the viewer. This will bring up the comparison viewer. When you are finished, click **Done** and then **Done Comparing**.

Hit Rates

Security Cloud Control enables you to evaluate the outcome of policy rules, on top of secure and scalable orchestration of policies, providing a simple visualization for more accurate policy analysis and an immediate, actionable pivot to root cause, all in a single pane from the cloud. The Hit Rates feature enables you to:

- Eliminate obsolete and never-matched policy rules, increasing security posture.
- Optimize firewall performance by instantly identifying bottlenecks as well as ensuring correct and efficient prioritization is enforced (for example, most triggered policy rule is prioritized higher).
- Maintain a history of Hit Rates information, even upon device or policy rule reset, for a configured data retention period (1 year).
- Strengthen validation of suspected shadow and unused rules based on actionable information. Removing doubt about update or delete.
- Visualize policy rule usage in the context of the entire policy, leveraging predefined time intervals (day, week, month, year) and scale of actual hits (zero, >100, >100k, etc.) to evaluate impact on packets traversing the network.

View Hit Rates of ASA Policies

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 2 Click the filter icon and pin it open.

Step 3 In the Hits area, click the various hit count filters to display which policies are being hit more or less often than others.

Search and Filter ASA Network Rules in the Access List

Search

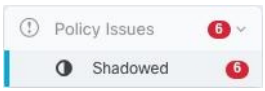
Use the search bar to search for names, keywords, or phrases in the names of the rules within the access list. Search is not case-sensitive.

Filter

Use the filter sidebar to find network policy issues. Filtering is not additive, each filter setting acts independently of the other.

Policy Issues

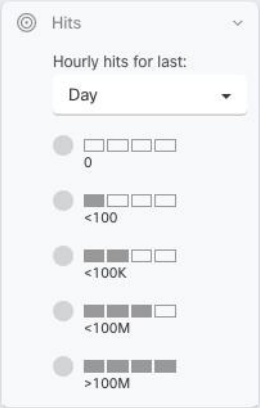
Security Cloud Control identifies network policies that contain shadow rules. The number of policies that contain shadow rules is indicated in the **Policy Issues** filter:



Security Cloud Control marks shadowed rules and network policies that contain them with the shadow badge shadow_badge.png on the network policies page. Click Shadowed to view all the policies containing shadow rules. See Shadow Rules for more information.

Hits

Use this filter to find rules across the access lists that have been triggered a number of times over a specified period.



Filter Use Cases

Find all rules that have zero hits

If you have rules without any hits, you can edit them to make them more effective or simply delete them.

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select 0 hits.

Find out how often rules in a network policy are being hit

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hits filters to see what category the different rules fall into.

Filter network policies by hit rate

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hit rate categories. Security Cloud Control displays the rules that are getting hit at the rate you specify.

Shadowed Rules

A network policy with shadowed rules is one in which at least one rule in the policy will never trigger because a rule that precedes it prevents the packet from being evaluated by the shadowed rule.

For example, consider these network objects and network rules in the "example" network policy:

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100
```

```
access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

No traffic is evaluated by this rule,

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

because the previous rule,

```
access-list example extended deny ip any4 object 02-50
```

denies any ipv4 address from reaching any address in the range 10.10.10.2 - 10.10.10.50.

Find Network Policies with Shadowed Rules

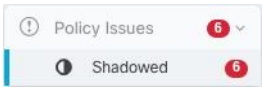
To find network policies with shadowed rules, use the network policies filter:

Procedure

Step 1 In the left pane, click **Policies** > **ASA** > **Access Policies**.

Step 2 Click the filter icon at the top of the ASA Access Policies table.

Step 3 In the Policy Issues filter, check **Shadowed** to view all the policies with shadowed rules.



Resolve Issues with Shadowed Rules

This is how Security Cloud Control displays the rules described in the "example" network policy above:

The rule on line 1 is marked with a shadow warning badge ⚠ because it's shadowing another rule in the policy. The rule on line 2 is marked as being shadowed ◑ by another rule in the policy. The action for the rule on line 2 is grayed-out because it's entirely shadowed by another rule in the policy. Security Cloud Control is able to tell you which rule in the policy shadows the rule in line 2.

The rule on line 3 can only be triggered some of the time. This is a partially shadowed rule. Network traffic from any IPv4 address trying to reach an IP address in the range 10.10.10.2-10.10.10.50 would never be evaluated because it would have already been denied by the first rule. However, any IPv4 address attempting to reach an address in the range 10.10.10.51-10.10.10.100 would be evaluated by the last rule and would be permitted.

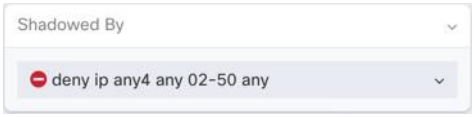
⚠

Caution Security Cloud Control does not apply a shadow warning badge ⚠ to partially shadowed rules.

Procedure

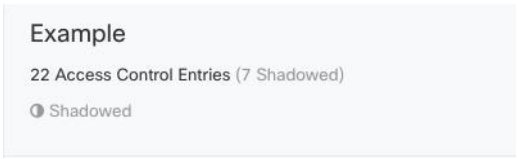
Step 1 Select the shadowed rule in the policy. In the example above, that means clicking on line 2.

Step 2 In the rule details pane, look for the **Shadowed By** area. In this example, the **Shadowed By** area for the rule in line 2 shows that it is being shadowed by the rule in line 1:



Step 3 Review the shadow*ing* rule. Is it too broad? Review the shadow*ed* rule. Do you really need it? Edit the shadow*ing* rule or delete the shadow*ed* rule.

Note By deleting shadowed rules, you reduce the number of access control entries (ACEs) on your ASA. This frees up space for the creation of other rules with other ACEs. Security Cloud Control calculates the number of ACEs derived from all the rules in a network policy and displays that total at the top of the network policy details pane. If any of the rules in the network policy are shadowed, it also lists that number.



Security Cloud Control also displays the number of ACEs derived from a single rule in a network policy and displays that information in the network policy details pane. Here is an example of that listing:

Step 4 Determine which devices use the policy by looking in the Devices area of the network policy details pane.

Step 5 Open the **Security Devices** page and **Deploy Changes** back to the devices affected by the policy change.

Network Address Translation

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private and not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of Network Address Translation (NAT) is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security-Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions-Overlapping IP addresses are not a problem when you use NAT.
- Flexibility-You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.
- Translating between IPv4 and IPv6 (Routed mode only)-If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

You can use Security Cloud Control to create NAT rules for many different use cases. Use the NAT rule wizard or these topics to create different NAT rules:

Order of Processing NAT Rules

Network Object NAT and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Table 3: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Twice NAT (ASA) Manual NAT (FTD)	Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, twice NAT rules are added to section 1.
Section 2	Network Object NAT (ASA) Auto NAT (FTD)	If a match in section 1 is not found, section 2 rules are applied in the following order: **1.** Static rules. **2.** Dynamic rules. **Within each rule type, the following ordering guidelines are used:** **1.** Quantity of real IP addressesâ€”From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. **2.** For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. **3.** If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, object "Arlington" is assessed before object "Detroit."
Section 3	Twice NAT (ASA) Manual NAT (FTD)	If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 172.16.1.0/24 (dynamic) (object Arlington)

The resultant ordering would be:

- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object Arlington)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 192.168.1.0/24 (dynamic)

Network Address Translation Wizard

The Network Address Translation (NAT) wizard helps you create NAT rules on your devices for these types of access:

- **Enable Internet Access for Internal Users**. You may use this NAT rule to allow users on an internal network to reach the internet.
- **Expose an Internal Server to the Internet**. You may use this NAT rule to allow people outside your network to reach an internal web or email server.

Prerequisites to "Enable Internet Access for Internal Users"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- If you want to allow only specific users to reach the internet, you need the subnet addresses for those users.

Prerequisites to "Expose an Internal Server to the Internet"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- The IP address of the server inside your network that you would like to translate to an internet-facing IP address.
- The public IP address you want the server to use.

What to do Next

See Create a NAT Rule by using the NAT Wizard, on page 47.

Create a NAT Rule by using the NAT Wizard

Before you begin

See Network Address Translation Wizard, on page 46 for the prerequisites needed to create NAT rules using the NAT wizard.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Use the filter and search fields to find the device for which you want to create the NAT rule.

Step 5 In the **Management** area of the details panel, click **NAT** NAT.

Step 6 Click  > **NAT Wizard**.

Step 7 Respond to the NAT Wizard questions and follow the on-screen instructions.

- The NAT Wizard creates rules with Network Objects. Either select an existing object from the drop-down menu, or create a new object with the create button + Create... .
- Before you can save the NAT rule, all IP addresses need to be defined as network objects.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Common Use Cases for NAT

Twice NAT and Manual NAT

Here are some common tasks that can be achieved using "Network Object NAT", also known as "Auto NAT":

- Enable a Server on the Inside Network to Reach the Internet Using a Public IP address, on page 48
- Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address, on page 49
- Make a Server on the Inside Network Available on a Specific Port of a Public IP Address, on page 50
- Translate a Range of Private IP Addresses to a Range of Public IP Addresses, on page 54

Network Object NAT and Auto NAT

Here is a common task that can be achieved using "Twice NAT", also know as "Manual NAT":

- Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface, on page 56

Enable a Server on the Inside Network to Reach the Internet Using a Public IP address

Use Case

Use this NAT strategy when you have a server with a private IP address that needs to be accessed from the internet and you have enough public IP addresses to NAT one public IP address to the private IP address. If you have a limited number of public IP addresses, see Make a Server on the Inside Network Available on a Specific Port of a Public IP Address (that solution may be more suitable).

Strategy

Your server has a static, private IP address, and users outside your network have to be able to reach your server. Create a network object NAT rule that translates the static private IP address to a static public IP address. After that, create an access policy that allows traffic from that public IP address to reach the private IP address. Finally, deploy these changes to your device.

Before you begin

Before you begin, create two network objects. Name one object *servername*_inside and the other object *servername*_outside. The *servername*_inside network object should contain the private IP address of your server. The *servername*_outside network object should contain the public IP address of your server. See Create Network Objects for instructions.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

a. Expand the Original Address menu, click **Choose**, and select the **servername_inside** object.

b. Expand the Translated Address menu, click **Choose**, and select the **servername_outside** object.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 For ASA, deploy a Network Policy rule or for FDM-managed device, deploy an access control policy rule to allow the traffic to flow from *servername*_inside to *servername*_outside.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

NAT rules created by this procedure:

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address

Use Case

Allow users and computers in your private network to connect to the internet by sharing the public address of your outside interface.

Strategy

Create a port address translation (PAT) rule that allows all the users on your private network to share the outside interface public IP address of your device.

After the private address is mapped to the public address and port number, the device records that mapping. When incoming traffic bound for that public IP address and port is received, the device sends it back to the private IP address that requested it.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + **Network Object NAT.**

Step 7 In section 1, **Type**, select **Dynamic.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **any** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions :

a. Expand the Original Address menu, click **Choose** and select the **any-ipv4** or **any-ipv6** object depending on your network configuration.

b. Expand the Translated Address menu, and select **interface** from the available list. Interface indicates to use the public address of the outside interface.

Step 10 For an FDM-managed device, in section 5, **Name**, enter a name for the NAT rule.

Step 11 Click **Save**.

Step 12 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

NAT rules created by this procedure:

```
object network any_network
nat (any,outside) dynamic interface
```

Make a Server on the Inside Network Available on a Specific Port of a Public IP Address

Use Case

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Prerequisites

Before you begin, create three separate network objects, one each for an FTP, HTTP, and SMTP server. For the sake of the following procedures, we call these objects **ftp-server-object**, **http-server-object**, and **smtp-server-object**. See Create Network Objects for instructions.

NAT Incoming FTP Traffic to an FTP Server

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  **> Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **ftp**-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **ftp, ftp.**

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here is the entry that is created and appears in the ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network ftp-object
host 10.1.2.27
```

NAT rule created by this procedure

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

NAT Incoming HTTP Traffic to an HTTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the http server. For the sake of this procedure, we will call the object, **http-object**. See Create Network Objects for instructions.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **http**-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **http**, http.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network http-object
host 10.1.2.28
```

NAT rule created by this procedure

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

NAT Incoming SMTP Traffic to an SMTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the smtp server. For the sake of this procedure, we will call the object, **smtp-object**. See Create Network Objects for instructions.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the smtp-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **smtp**, **smtp.**

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network smtp-object
host 10.1.2.29
```

NAT rule created by this procedure

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

Translate a Range of Private IP Addresses to a Range of Public IP Addresses

Use Case

Use this approach if you have a group of specific device types, or user types, that need to have their IP addresses translated to a specific range so that the receiving devices (the devices on the other end of the transaction) allow the traffic in.

Translate a Pool of Inside Addresses to a Pool of Outside Addresses

Before you begin

Create a network object for the pool of private IP addresses you want to translate and create a network object for the pool of public addresses you want to translate those private IP addresses into.

For the ASA, the "original address" pool, (the pool of private IP addresses you want to translate) can be a network object with a range of addresses, a network object that defines a subnet, or a network group that includes all the addresses in the pool. For the FTD, the "original address" pool can be a network object that defines a subnet or a network group that includes all the addresses in the pool.

Note For the ASA , the network group that defines the pool of "translated address" cannot be a network object that defines a subnet.

When creating these address pools, use Create or Edit ASA Network Objects and Network Groups for instructions.

For the sake of the following procedure, we named the pool of private addresses, **inside_pool** and name the pool of public addresses, **outside_pool.**

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT**.

Step 7 In section 1, **Type**, select **Dynamic** and click **Continue**.

Step 8 In section 2, **Interfaces**, set the source interface to **inside** and the destination interface to **outside**. Click **Continue**.

Step 9 In section 3, **Packets**, perform these tasks:

- For the Original Address, click **Choose** and then select the **inside_pool** network object (or network group) you made in the prerequisites section above.
- For the Translated Address, click **Choose** and then select the **outside_pool** network object (or network group) you made in the prerequisites section above.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

These are the entries that would appear in an ASA's saved configuration file as a result of these procedures.

Note This does not apply to FDM-managed devices.

Objects created by this procedure

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

NAT rules created by this procedure

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface

Use Case

Use this Twice NAT use case to enable site-to-site VPN.

Strategy

You are translating a pool of IP addresses to itself so that the IP addresses in one location on the network arrives unchanged in another.

Create a Twice NAT Rule

Before you begin

Create a network object or network group that defines the pool of IP addresses you are going to translate to itself. For the ASA, the range of addresses can be defined by a network object that uses an IP address range, a network object that defines a subnet, or a network group object that includes all the addresses in the range.

When creating the network objects or network groups, use Create or Edit ASA Network Objects and Network Groups for instructions.

For the sake of the following procedure, we are going call the network object or network group, Site-to-Site-PC-Pool.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Twice NAT.**.

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, make these changes:

- Expand the Original Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.
- Expand the Translated Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 For an ASA, create a crypto map. See CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide and review the chapter on LAN-to-LAN IPsec VPNs for more information on creating a crypto map.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

These are the entries that would appear in an ASA's saved configuration file as a result of these procedures.

Note This does not apply to FDM-managed devices.

Objects created by this procedure

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

NAT rules created by this procedure

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

ASA Templates

Templates enable users to construct a device/service configuration generically, so that they can apply that configuration to others that have been grouped together. These templates provide a single location to make a change in order to impact the many implementers that are grouped together.

ASA Template Parameters

When creating a new template, you may want to model it after a particular device. Security Cloud Control offers the ability to set template parameters based on selected fields of text within the configuration of the device that the template is modeled after. Parameters can be created, set up from existing parameters, and searched for within the template parameters view.

Note If you opt to import a configuration for an ASA template, the configuration must be in a JSON format.

Create New Parameters

Procedure

Step 1 With an existing device onboarded, navigate to the **Templates** tab at the top of Security Cloud Control.

Step 2 Either select **New Template** or **Manage Templates.**

Step 3 Choose the desired configuration to create a parameter.

Step 4 Name the template by typing in the Name field at the top of the screen.

Step 5 Select the desired text field to add a parameter to.

Step 6 Give the parameter a description, add a value, and any necessary note.

Step 7 Click **Save** next to the Name field to save the parameter.

Step 8 You can then review the template by clicking **Review Template.**

You now have a saved parameter that gets applied to all future devices that are onboarded using this template.

Create a New ASA, ISR, or ASR Template

Base Configuration

Start with a known ASA, ISR, or ASR base configuration. Choose the desired configuration to begin parameterization of the template. Parameterization involves selecting fields or attributes within a configuration file and identifying a list of values which will be selected on configuration file instantiation.

Note If you opt to import a configuration for an ASA template, the configuration must be in a JSON format.

Add Parameters

With the selection of a base configuration the parameterization process can begin. From the configuration editor, select the desired field for parameterization. Note that the selected string is enclosed in double brackets. From the left pane, the parameter can be renamed, a description added, and multiple values added. Selecting **Allow Custom Value** allows for custom values to be set on instantiation. Otherwise, only the identified values are selectable.

Once parameterization is completed, identify a name for the template, and click **Save**.

Read more on parameterization ASA Template Parameters.

Review

Once a template has been saved, click **Review** to move to the review process. In review, the template can be exported as-is, including the parameterized values. Note that this is not necessarily a valid configuration but provides a means to review the template as it is stored in Security Cloud Control. The template can also be edited by clicking **Edit**, if needed. The **Diff** button can demonstrate the differences between the saved template and the most recent edits.

Generate ASA Configurations from Templates

Create a Configuration from a Template

Select the **Config from Template** button to begin the process of generating a custom configuration from a template. Available templates are listed, select the chosen template and click **Choose Template**.

In most cases, templates will contain parameterized values which must be set on **Export** to provide the customized configuration. From the left hand pane, select each parameter and value as desired for this configuration. Notice the values are demonstrated in the editor. These are the values that will replace the

parameter on export. With all parameter values set, click on the **Export** button to export the configuration and download. If the template contains no parameterized values, click the **Export** button to export the configuration as is.

Manage ASA Templates

The Manage Templates view gives you the ability to visualize all of your existing templates as well as edit and delete them. Parameterization and value configuration can be modified while editing templates. Simply hover over an existing template and select **Edit** to make changes.

Edit Templates

Once in the edit view:

- Add parameters by double-clicking or highlighting text in the editor.
- Describe the parameter by typing in the description text box. Then click **Add Value**.
- Provide a value and write a note. Click **Add**.
- When you are done, click **Save**.
- You can now review the template by clicking **Review Template**.
  - You can compare the files by clicking **Diff**.
  - To export the template, click **Export**.

API Tokens

Developers use Security Cloud Control API tokens when making Security Cloud Control REST API calls. The API token must be inserted in the REST API authorization header for a call to succeed. API tokens are "long-lived" access tokens which do not expire; however, you can renew and revoke them.

You can generate API tokens from within Security Cloud Control. These tokens are only visible immediately after they're generated and for as long as the General Settings page is open. If you open a different page in Security Cloud Control and return to the General Settings page, the token is no longer visible, although it is clear that a token has been issued.

Individual users can create their own tokens for a particular tenant. One user cannot generate a token on behalf of another. Tokens are specific to an account-tenant pair and cannot be used for other user-tenant combinations.

API Token Format and Claims

The API token is a JSON Web Token (JWT). To learn more about the JWT token format, read the Introduction to JSON Web Tokens.

The Security Cloud Control API token provides the following set of claims:

- **id** - user/device uid
- **parentId** - tenant uid
- **ver** - the version of the public key (initial version is 0, for example, **cdo_jwt_sig_pub_key.0**)

- **subscriptions** - Security Services Exchange subscriptions (optional)
- **client_id** - "**api-client**"
- **jti** - token id

Migrating an ASA Configuration to an FDM-Managed Device Template

Attention Firepower Device Manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. Send a request to the support team to enable this platform.

Security Cloud Control helps you migrate your ASA to an FDM-managed device. Security Cloud Control provides a wizard to help you migrate these elements of the ASA's running configuration to an FDM-managed device template:

- Access Control Rules (ACLs)
- Interfaces
- Network Address Translation (NAT) rules
- Network objects and network group objects
- Routes
- Service objects and service group objects
- Site-to-site VPN

Once these elements of the ASA running configuration have been migrated to an FDM-managed device template, you can then apply the FDM template to a new FDM-managed device that is managed by Security Cloud Control. The FDM-managed device adopts the configurations defined in the template, and so, the FDM-managed device is now configured with some aspects of the ASA's running configuration.

Other elements of the ASA running configuration are not migrated using this process. Those other elements are represented in the FDM-managed device template by empty values. When the template is applied to an FDM-managed device, we apply values we migrated to the new FDM-managed device and ignore the empty values. Whatever other default values the new FDM-managed device has, it retains. Those other elements of the ASA running configuration that we did not migrate, will need to be recreated on the FDM-managed device outside the migration process.

See Migrating an ASA to an FDM-Managed Device Using Cisco Security Cloud Control for a full explanation of the process of migrating an ASA to an FDM-managed device using Security Cloud Control.

Manage ASA Certificates

Digital certificates provide digital identification for authenticating devices and individual users. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. For more information on digital certificates, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Certificate Authorities (CAs) are trusted authorities that "sign" certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs also issue identity certificates.

- **Identity Certificate** — Identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate. CAs issue identity certificates, which are certificates for specific systems or hosts.
- **Trusted CA Certificate** — Trusted CA certificates are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. A trusted CA certificate is self-signed and called a root certificate.

The Remote Access VPN uses digital certificates for authenticating secure gateways and AnyConnect clients (endpoints) to establish a secure VPN connection. For more information, see Remote Access VPN Certificate-Based Authentication.

Guidelines for Certificate Installation

Read the following guidelines for certificate installation on ASA:

- Certificate can be installed on a single or multiple ASA devices simultaneously.
- Only one certificate can be installed at a time.
- Certificate can be installed only on a live ASA device and not on a modal device.

Install ASA Certificates

You must upload the digital certificates as trustpoint objects and install them on the ASA devices managed by Security Cloud Control.

Note Ensure that the ASA device has no out-of-band changes, and all staged changes have been deployed.

The following lists the digital certificates and formats supported by Security Cloud Control:

- Identity Certificate can be installed using the following methods:
  - PKCS12 file import.
  - Self-Signed certificate
  - Certificate Signing Request (CSR) import.

- Trusted CA Certificate can be installed using PEM or DER format.

Watch the screencast demonstrates the steps for installing certificates on ASA using Security Cloud Control. It also shows steps for modifying, exporting, and deleting installed certificates.

Supported Certificate Formats

- PKCS12: PKCS#12, P12, or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as **.pfx** and **.p12**.
- PEM: PEM (originally “Privacy Enhanced Mail”) files contain ASCII (or Base64) encoding data and the certificate files can be in .pem, .crt, .cer, or .key formats. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements.
- DER: DER (Distinguished Encoding Rules) format is simply a binary form of a certificate instead of the ASCII PEM format. It sometimes has a file extension of **.der**, but it often has a file extension of **.cer**, so the only way to tell the difference between a DER .cer file and a PEM .cer file is to open it in a text editor and look for the BEGIN/END statements. Unlike PEM, DER-encoded files do not contain plain text statements such as -----BEGIN CERTIFICATE-----.

Trustpoints Screen

After onboarding the ASA device into Security Cloud Control, on the **Security Devices** tab, select the ASA device and in the **Management** pane on the left, click **Trustpoints**.

In the **Trustpoints** tab, you'll see the certificates that are already installed on the device.

- The "Installed" status indicates that the corresponding certificate is installed successfully on the device.
- The "Unknown" status indicates that the corresponding certificate doesn't contain any information. You need to remove and upload it again with the correct details. Security Cloud Control discovers all the unknown certificates as trusted CA certificates.
- Click the row that shows "Installed" to view certificate details on the right pane. Click **more** to see additional details of the selected certificate.
- An installed Identity Certificate can be exported in PKCS12 or PEM format and imported into other ASA devices. See Exporting an Identity Certificate.
- Only the advanced settings can be modified on an installed certificate.
  - Click **Edit** to modify the advanced settings.
  - After making the changes, click **Send** to install the updated certificate.

Install an Identity Certificate Using PKCS12

You can select an existing trustpoint object created for PKCS12 format and install it on the ASA device. You can also create a new trustpoint object from the installation wizard and install the certificate on the ASA device.

Before you begin

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Step 2 To install an identity certificate on a single ASA device, do the following:

a) Click the **Devices** tab.
b) Click the **ASA** tab and select an ASA device.
c) In the **Management** pane on the right, click **Trustpoints**.
d) Click **Install**.

Note You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

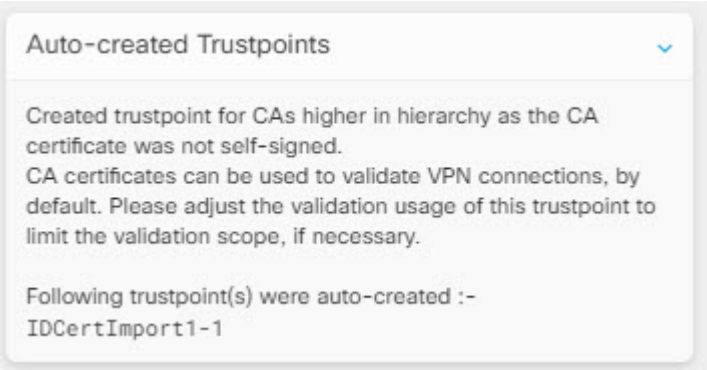
Step 3 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object. For more information, see Adding an Identity Certificate Object Using PKCS12.
- **Choose** to select Certificate Enrollment Object of the PKCS type.

Step 4 Click **Send**.

This installs the certificate on the ASA device

Note If you are importing a PKCS12 certificate that has intermediate CAs installed on it, ASA automatically creates and installs trustpoint objects on the device for every intermediate CA certificate that is not installed already. When you click on the identity certificate, you'll see a message on the right pane, as shown in the following example.



Install a Certificate Using Self-Signed Enrollment

You can select an existing trustpoint object created for a self-signed certificate and install it on the ASA device. You can also create a new trustpoint object from the installation wizard and install the certificate on the ASA device.

Before you begin

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Step 2 To install an identity certificate on a single ASA device, do the following:

a) Click the **Devices** tab.
b) Click the **ASA** tab and select an ASA device.
c) In the **Management** pane on the right, click **Trustpoints**.
d) Click **Install**.

Note You can also install a signed certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Step 3 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object. For more information, see Adding an Identity Certificate Object Using PKCS12.
- **Choose** to select a Certificate Enrollment Object of the type Self-Signed..

Step 4 Click **Send**.

For self signed enrollment type trustpoints, the Issuer Common Name status will always be the ASA device since the managed device is acting as its own CA and does not need a CA certificate to generate its own Identity Certificate.

Manage a Certificate Signing Request (CSR)

You must first generate a CSR request and then get this request signed by a trusted Certificate Authority (CA). Then, you can install the signed identity certificate issued by the CA on the ASA device.

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

The following diagram depicts the workflow for generating CSR and installing a certified issued certificate in ASA:

Generate a CSR Request

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 To install an identity certificate on a single ASA device, do the following:

Step 5 Click **Install**.

Step 6 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint CSR object. For more information, see Adding an Identity Certificate Object for Certificate Signing Request (CSR).
- **Choose**to select the CSR request trustpoint that is already created..

Step 7 Click **Send**.

This generates an unsigned Certificate Signing Request (CSR).

Step 8 Click the copy icon copy_icon.png to copy the CSR details. You can also download the CSR request in ".csr" file format.

Step 9 Click **OK**.

Step 10 Submit the certificate signing request (CSR) to the Certificate Authority to sign the certificate.

Install a Signed Identity Certificate Issued by a Certificate Authority

Once the CA issues the signed certificate, install it on the ASA device

Procedure

Step 1 In the **Trustpoint** screen, click the CSR request with the **Status** as "Awaiting Signed Certificate Install" and in the **Actions** pane on the right, click **Install Certified ID Certificate**.

Step 2 Upload the signed certificate received from the CA. You can drag and drop the file or paste its contents in the provided field. The trustpoint commands are generated based on the trustpoint you selected.

Step 3 Click **Send**.

This installs the signed identity certificate to the ASA device. Installing certificates will immediately deploy changes to the device.

Note You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Install a Trusted CA Certificate in ASA

Before you begin

- Read the Guidelines for Certificate Installation.
- ASA must be “Synced” state and “Online”.

Procedure

Step 1 In the navigation menu, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 To install an identity certificate on a single ASA device, do the following:

a) Select an ASA device and in the **Management** pane on the right, click **Trustpoints**.

b) Click **Install**.

Note You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Step 5 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object. For more information, see Adding a Trusted CA Certificate Object.
- **Choose**select a Trusted Certificate Authority Object.

Step 6 Click **Send**.

This installs the trusted CA file on the ASA device.

Export an Identity Certificate

You can export and import the keypair and issued certificates associated with a trustpoint in PKCS12 or PEM format. This format is useful to manually duplicate a trustpoint configuration on a different ASA.

Procedure

Step 1 In the navigation menu, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA**.

Step 4 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 5 Click the identity certificate to export the certificate configuration. Alternatively, you can search for the certificate by entering its name in the search field.

Step 6 In the **Actions** pane on the right, click **Export Certificate**.

Step 7 Choose the certificate format by clicking the **PKCS12 Format** or the **PEM Format**.

Step 8 Enter the encryption passphrase used to encrypt the PKCS12 file for export.

Step 9 Confirm the encryption passphrase.

Step 10 Click **Export** to export the certificate configuration.

An information dialog box appears, informing you that the certificate configuration file has been successfully exported to the location that you specified.

What to do next

If you want to view the downloaded identity certificate, execute the following commands in the directory where the certificate was downloaded:

1. To decode certificate in base64 format:

```
openssl base64 -d -in <file_name>.p12 -out <file_name>_b64.p12
```

2. To view certificate:

```
openssl pkcs12 -in <file_name>_b64.p12 -passin pass:<password>
```

Edit an Installed Certificate

You can modify only the advanced options of the installed certificate.

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab.

Step 4 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 5 Click the certificate to modify and in the **Actions** pane on the right, click **Edit**.

Step 6 Modify the required parameters and click **Save**.

Delete an Existing Certificate from ASA

You can delete a certificate one after another. After deleting a certificate, it cannot be restored.

Procedure

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

Step 2 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 3 Click the certificate to be deleted and in the **Actions** pane on the right, click **Remove**.

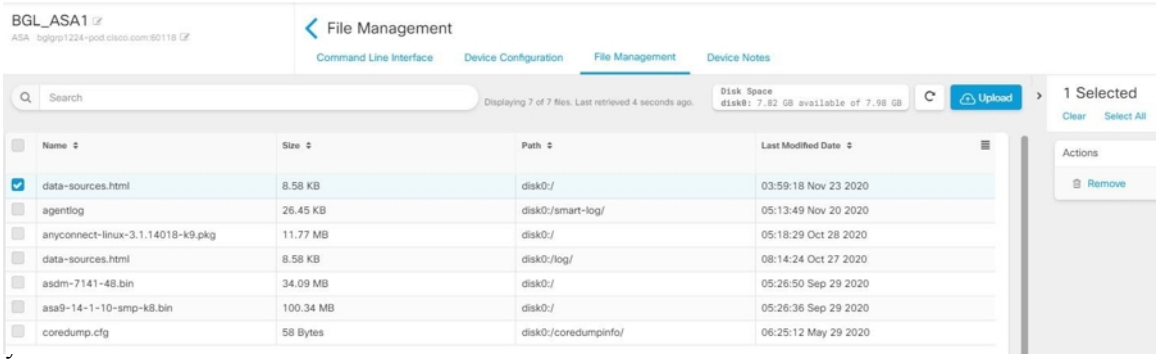
Step 4 Click **OK** to remove the selected certificate.

ASA File Management

Security Cloud Control provides the file management tool to help you perform basic file management tasks such as viewing, uploading, or deleting files present on the ASA device's flash (disk0) space.

Note You cannot manage files present on disk1.

The File Management screen lists all the files present on the device's flash (disk0). On a successful file upload, you can click the refresh icon to see the file. By default, this screen refreshes automatically every 10 minutes. The **Disk Space** field shows the amount of disk space on the disk0



You can upload the AnyConnect image to single or multiple ASA devices. After a successful upload, the AnyConnect image is associated with the RA VPN configuration on the selected ASA devices. This helps you to upload the newly released AnyConnect package to multiple ASA devices simultaneously.

Upload File to the Flash System

Security Cloud Control supports only URL based file upload from the remote server. The supported protocols for uploading the file are HTTP, HTTPS, TFTP, FTP, SMB, or SCP. You can upload any files such as the AnyConnect software images, DAP.xml, data.xml, and host scan image files to a single or multiple ASA device.

Note Security Cloud Control doesn't upload the file to selected ASA devices if the remote server's URL path is invalid or for any issues that may occur. You can navigate to the device **Workflows** for more details.

Suppose the device is configured for High Availability, Security Cloud Control uploads the file to the standby device first, and only after a successful upload, the file is uploaded to the active device. The same behavior applies during the file removal process.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazon/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://[redacted]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://root:cisco123@10.10.16.6//root/events_send.py

Before You Begin

- Make sure that the remote server is accessible from the ASA device.
- Make sure that the file is already uploaded to the remote server.
- Make sure that there is a network route from the ASA device to that server.
- If FQDN is used in the URL, make sure that DNS is configured.
- The remote server's URL must be a direct link without prompting for authentication.
- If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Note If you upload a file to an ASA that is configured as a peer in a failover, Security Cloud Control does not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for Security Cloud Control to recognize the file in both devices.

Upload File to a Single ASA Device

Use this procedure to upload a file to a single ASA device.

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 In the **Management** pane on the right, click **File Management**. You can view available disk space and the files present on the ASA device.

Step 5 Click the **Upload** button on the right.

Step 6 In the **URL link**, specify the server's path where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:**/DAPFiles/dap.xml" in the field.

Note You can view the directories present in the disk0 folder by executing the **dir** command in the Security Cloud Control ASA CLI interface.

Step 7 If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled. **Note**: This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, Security Cloud Control associates the AnyConnect file to the RA VPN configuration on the selected ASA device after a successful upload.

Step 8 Click **Upload**. Security Cloud Control uploads the file to the device.

Step 9 If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 5, Deploy Configuration Changes from Security Cloud Control to ASA.

What to do next

You don't have to deploy the configuration changes on the device.`

Upload File to Multiple ASA Devices

Use this procedure to upload a file to multiple ASA devices at the same time.

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select multiple ASA devices to perform a bulk upload.

Step 4 In the **Device Actions** pane on the right, click **Upload File**. Note: The **Upload File** link appears if ASA devices are online.

Step 5 In the **URL link**, specify the server's paths where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:**/DAPFiles/dap.xml" in the field.

Note You can view the directories present in the disk0 folder by executing the **dir** command in the Security Cloud Control ASA CLI interface.

Step 6 If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled.

Note This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, Security Cloud Control associates the AnyConnect file to the RA VPN configuration on the selected ASA devices after a successful upload.

Step 7 Click **Upload**.

Step 8 If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 4, Deploy Configuration Changes from Security Cloud Control to ASA.

What to do next

You can view the progress of uploading the file on individual devices. Select the ASA device, and in the **Management** pane on the right, click **File Management**. If the file upload is in progress, wait for the operation to complete.

You don't have to deploy the configuration changes on the device.`

Remove Files from ASA

You are not allowed to remove AnyConnect files associated with the RA VPN configuration. You have to disassociate the AnyConnect file from the corresponding RA VPN configuration and then remove the file from the File Management tool.

Note If you upload a file to an ASA that is configured as a peer in a failover, Security Cloud Controldoes not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for Security Cloud Control to recognize the file in both devices.

The remove operation deletes the selected files permanently from the flash memory. A message appears when deleting files asking for confirmation. Use the following procedure to remove files from a selected ASA device:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select an ASA device.

Step 4 In the **Management** pane on the right, click **File Management**.

Step 5 Select the files you want to remove, and under **Actions** on the right, click **Remove**. A maximum of 25 files can be selected. If Security Cloud Control fails to remove some files, you can see the device **Workflows** to determine the removed and retained files.

Step 6 If you have chosen to remove the AnyConnect package, Deploy Configuration Changes from Security Cloud Control to ASA.

Managing ASAs with Pre-existing High Availability Configuration

Configuration Changes Made to ASAs in Active-Active Failover Mode

When Security Cloud Control) changes an ASA's running configuration with the one staged on Security Cloud Control, or when it changes the configuration on Security Cloud Control with the one stored on the ASA, it attempts to change only the relevant lines of the configuration file if that aspect of the configuration can be managed by the Security Cloud Control GUI. If the desired configuration change cannot be made using the Security Cloud Control GUI, Security Cloud Control attempts to overwrite the entire configuration file to make the change.

Here are two examples:

- You *can* create or change a network object using the Security Cloud Control GUI. If Security Cloud Control needs to deploy that change to an ASA's configuration, it overwrites the relevant lines of the running configuration file on the ASA when the change occurs.
- You *cannot* create a new ASA user using the Security Cloud Control GUI. If a new user is added to the ASA using the ASA's ASDM or CLI, when that out-of-band change is accepted and Security Cloud Control updates the stored configuration file, Security Cloud Control attempts to overwrite that ASA's entire configuration file staged on Security Cloud Control.

These rules are not followed when the ASA is configured in active-active failover mode. When Security Cloud Control manages an ASA configured in active-active failover mode, Security Cloud Control cannot always deploy all configuration changes from itself to the ASA or read all configuration changes from the ASA into itself. Here are two instances in which this is the case:

- **Changes to an ASA's configuration file made in Security Cloud Control, that Security Cloud Control does not otherwise support in the Security Cloud Control GUI, cannot be deployed to the ASA**. Also, a combination of changes made to the configuration file that Security Cloud Control does not support, along with changes made to the configuration file that Security Cloud Control does support, cannot be deployed to the ASA. In both cases, you receive the error message, "Security Cloud Control does not support replacing full configurations for devices in failover mode at this time. Please click Cancel and apply changes to the device manually." Along with the message in the Security Cloud Control interface, you see a Replace Configuration button that is disabled.
- **Out-of-band changes made to an ASA configured in active-active failover mode will not be rejected by Security Cloud Control**. If you make an out-of-band change to an ASA's running configuration, the ASA gets marked with "Conflict Detected" on the **Security Devices** page. If you review the conflict and try to reject it, Security Cloud Control blocks that action. You receive the message, "Security Cloud Control does not support rejecting out-of-band changes for this device. Either this device is running an unsupported software version or is a member of a active/active failover pair. Please proceed to accept the out-of-band changes by clicking Continue."

Caution If you find yourself having to accept out-of-band changes from the ASA, any configuration changes staged on Security Cloud Control, but not yet deployed to the ASA, will be overwritten and lost.

Security Cloud Control does support configuration changes made to an ASA in failover mode when those changes are supported by the Security Cloud Control GUI.

Related Information:

Configure DNS on ASA

Use this procedure to configure a domain name server (DNS) on each of your ASAs.

Prerequisites

- The ASA must be able to reach the internet.
- Before you begin, gather this information:
  - The name of the ASA interface that can reach the DNS server; for example, inside, outside, or dmz.
  - The IP address of the DNS server your organization uses. If you don't maintain your own DNS server, you can use Cisco Umbrella. The IP address for Cisco Umbrella is 208.67.220.220.

Procedure

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab and select all the ASAs on which you want to configure DNS.

Step 4 In the Actions pane to the right, select **Command Line Interface**.

Step 5 Click the CLI macro favorites star.

Step 6 Select the **Configure DNS** macro in the Macros panel.

Step 7 Se;ect **>_View Parameters** and in the parameters column, fill in the values for these parameters:

- IF_Name - The name of the ASA interface that can reach the DNS server.
- IP_ADDR - The IP address of the DNS server your organization uses.

Step 8 Click **Send to devices**.

Security Cloud Control Command Line Interface

Security Cloud Control provides users with a command line interface (CLI) for managing ASA devices. Users can send commands to a single device or to multiple devices simultaneously.

Related Information:

- For detailed ASA CLI documentation, see ASA Command Line Interface Documentation, on page 87.

Using the Command Line Interface

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Use the device tabs and filter button to find the device you want to manage using the command line interface (CLI).

Step 4 Select the device.

Step 5 In the **Device Actions** pane, click **>_Command Line Interface.**

Step 6 Click the **Command Line Interface** tab.

Step 7 Enter your command, or commands, in the command pane and click **Send.** The device's response to the command(s) are displayed below in the "response pane."

Note If there are limitations on the commands you can run, those limitations are listed above the command pane.

Related Topics

Entering Commands in the Command Line Interface, on page 74

Entering Commands in the Command Line Interface

A single command can be entered on a single line or several commands can be entered sequentially on several lines and Security Cloud Control will execute them in order. The following ASA example sends a batch of commands which creates three network objects and a network object group that contains those network objects.

Entering ASA **device Commands**: Security Cloud Control executes commands in ASA's Global Configuration mode.

Long Commands: If you enter a very long command, Security Cloud Control attempts to break up your command into multiple commands, so that they can all be run against the API. If Security Cloud Control is unable to determine a proper separation of your command, it will prompt you for a hint on where to break the list of commands. For example:

```
Error: Security Cloud Control attempted to execute a portion of this command with a length
that exceeded 600 characters. You can give a hint to Security Cloud Control at where a
proper command separation point is by breaking up your list of commands with an additional
empty line between them.
```

If you receive this error:

Procedure

Step 1 Click the command in the CLI history pane that caused error. Security Cloud Control populates the command box with the long list of commands.

Step 2 Edit the long list of commands by entering an empty line after groups of related commands. For example, add an empty line after you define a list of network objects and add them to a group like in the example above. You may want to do this at a few different points in the list of commands.

Step 3 Click **Send**.

Work with Command History

After you send a CLI command, Security Cloud Control records that command in the history pane on the **Command Line Interface** page. You can rerun the commands saved in the history pane or use the commands as a template:

Procedure

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

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

Step 3 Click the appropriate device type tab.

Step 4 Click **>_Command Line Interface**.

Step 5 Click the clock icon to expand the history pane if it is not already expanded.

Step 6 Select the command in the history pane that you want to modify or resend.

Step 7 Reuse the command as it is or edit it in the command pane and click **Send**. Security Cloud Control displays the results of the command in the response pane.

Note Security Cloud Control displays the `Done!` message in the response pane in two circumstances:

- After a command has executed successfully.
- When the command has no results to return. For example, you may issue a show command with a regular expression searching for a configuration entry. If there is no configuration entry that meets the criteria of the regular expression, Security Cloud Control returns `Done!`.

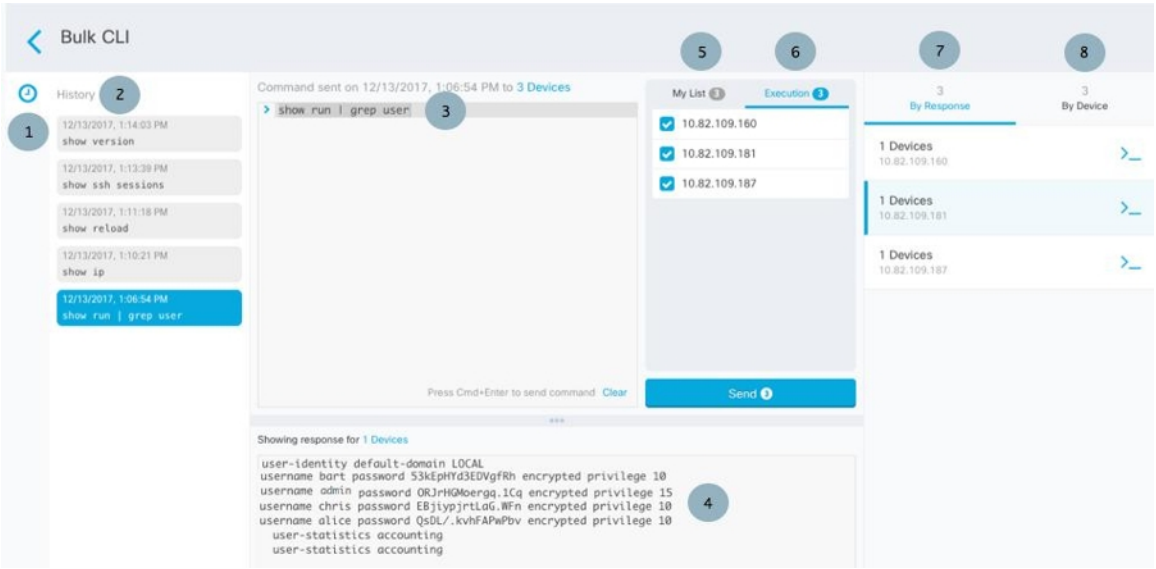
Bulk Command Line Interface

Security Cloud Control offers users the ability to manage Secure Firewall ASA, FDM-managed Threat Defense, SSH, and Cisco IOS devices using a command-line interface (CLI). Users can send commands to a single device or to multiple devices of the same kind simultaneously. This section describes sending CLI commands to multiple devices at once.

Related Information:

- For detailed documentation on the ASA CLI documentation, see ASA Command Line Interface Documentation, on page 87.

Bulk CLI Interface



Note Security Cloud Control displays the **Done!** message in two circumstances:

- After a command has executed successfully without errors.
- When the command has no results to return. For example, you may issue a show command with a regular expression searching for a certain configuration entry. If there is no configuration entry that meets the criteria of the regular expression, Security Cloud Control returns **Done!**.

Number	Description
1	Click the clock to expand or collapse the command history pane.
2	Command history. After you send a command, Security Cloud Control records the command in this history pane so you can return to it, select it, and run it again.

Number	Description
3	Command pane. Enter your commands at the prompt in this pane.
4	Response pane. Security Cloud Control displays the device's response to your command as well as Security Cloud Control messages. If the response was the same for more than one device, the response pane displays the message "Showing Responses for X devices." Click X devices and Security Cloud Control displays all the devices that returned the same response to the command. **Note** Security Cloud Control displays the **Done!** message in two circumstances: • After a command has executed successfully without errors. • When the command has no results to return. For example, you may issue a show command with a regular expression searching for a certain configuration entry. If there is no configuration entry that meets the criteria of the regular expression, Security Cloud Control returns **Done!**.
5	**My List** tab displays the devices you chose from the **Inventory** table and allows you to include or exclude devices you want to send a command to.
6	The **Execution** tab, highlighted in the figure above, displays the devices in the command that is selected in the history pane. In this example, the show run | grep user command is selected in the history pane and the Execution tab shows that it was sent to 10.82.109.160, 10.82.109.181, and 10.82.10.9.187.
7	Clicking the **By Response** tab shows you the list of responses generated by the command. Identical responses are grouped together in one row. When you select a row in the By Response tab, Security Cloud Control displays the response to that command in the response pane.
8	Clicking the **By Device** tab displays individual responses from each device. Clicking one of the devices in the list allows you to see the response to the command from a specific device.

Send Commands in Bulk

Procedure

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

Step 2 Click the **Devices** tab to locate the devices.

Step 3 Select the appropriate device tab and use the filter button to find the devices you want to configure using the command line interface.

Step 4 Select the devices.

Step 5 in the **Device Actions** pane, click **>_Command Line Interface**.

Step 6 You can check or uncheck devices you want to send the commands to in the **My List** field.

Step 7 Enter your commands in the command pane and click **Send**. The command output is displayed in the response pane, the command is logged in the Change Log, and the command Security Cloud Control records your command in the History pane in the Bulk CLI window.

Note A command will succeed on selected ASA devices that are synced and may fail on devices that are not synced. If any of the selected ASA devices are not synced, only the following commands are allowed: `show, ping, traceroute, vpn-sessiondb, changeto, dir, write, and copy`.

Work with Bulk Command History

After you send a bulk CLI command, Security Cloud Control records that command in the Bulk CLI Interface history page. You can rerun the commands saved in the history pane or use the commands as a template. The commands in the history pane are associated with the original devices on which they were run.

Procedure

Step 1 In the navigation pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate devices.

Step 3 Click the appropriate device type tab and click the filter icon to find the devies you want to configure.

Step 4 Select the devices.

Step 5 Click **Command Line Interface**.

Step 6 **Select** the command in the History pane that you want to modify or resend. Note that the command you pick is associated with specific devices and not necessarily the ones you chose in the first step.

Step 7 Look at the My List tab to make sure the command you intend to send will be sent to the devices you expect.

Step 8 Edit the command in the command pane and click **Send**. Security Cloud Control displays the results of the command in the response pane.

Note A command will succeed on selected ASA devices that are synced and may fail on devices that are not synced. If any of the selected ASA devices are not synced, only the following commands are allowed: `show, ping, traceroute, vpn-sessiondb, changeto, dir, write, and copy`.

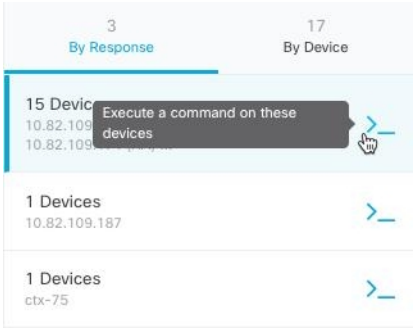
Work with Bulk Command Filters

After you run a bulk CLI command you can use the **By Response** filter and the **By Device** filter to continue to configure the devices.

By Response Filter

After running a bulk command, Security Cloud Control populates the **By Response** tab with a list of responses returned by the devices that were sent the command. Devices with identical responses are consolidated in a single row. Clicking a row in the **By Response** tab displays the response from the device(s) in the response pane. If the response pane shows a response for more than one device, it displays the message "Showing

Responses for X devices." Click **X devices** and Security Cloud Control displays all the devices that returned the same response to the command.



To send a command to the list of devices associated with a command response, follow this procedure:

Procedure

Step 1 Click the command symbol in a row in the **By Response** tab.

Step 2 Review the command in the command pane and click **Send** to resend the command or click **Clear** to clear the command pane and enter a new command to send to the devices and then click **Send**.

Step 3 Review the responses you receive from your command.

Step 4 If you are confident that the running configuration file on the devices you chose reflects your change, type `write memory` in the command pane and click **Send**. This saves your running configuration to the startup configuration.

By Device Filter

After running a bulk command, Security Cloud Control populates the the Execution tab and the **By Device** tab with the list of devices that were sent the command. Clicking a row in the **By Device** tab displays the response for each device.

To run a command on that same list of devices, follow this procedure:

Procedure

Step 1 Click the **By Device** tab.

Step 2 Click **>_Execute a command on these devices**.

Step 3 Click **Clear** to clear the command pane and enter a new command.

Step 4 In the My List pane, specify the list of devices you want to send the command to by checking or unchecking individual devices in the list.

Step 5 Click **Send**. The response to the command is displayed in the response pane. If the response pane shows a response for more than one device, it displays the message "Showing Responses for X devices." Click X devices and Security Cloud Control displays all the devices that returned the same response to the command.

Step 6 If you are confident that the running configuration file on the devices you chose reflects your change, type `write memory` in the command pane and click **Send**.

Command Line Interface Macros

A CLI macro is a fully-formed CLI command ready to use, or a template of a CLI command you can modify before you run it. All macros can be run on one or more ASA devices simultaneously.

Use CLI macros that resemble templates to run the same commands on multiple devices at the same time. CLI macros promote consistency in your device configurations and management. Use fully-formed CLI macros to get information about your devices. There are different CLI macros that are immediately available for you to use on your ASA devices.

You can create CLI macros for monitoring tasks that you perform frequently. See Create a CLI Macro from a New Command for more information.

CLI macros are system-defined or user-defined. System-defined macros are provided by Security Cloud Control and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted.

Note You can only create macros for a device once it has been onboarded to Security Cloud Control.

Using the ASA as an example, if you want to find a particular user on one of your ASAs, you could run this command:

```
show running-config | grep username
```

When you run the command, you would replace *username* with the username of the user you are searching for. To make a macro out of this command, use the same command and put curly braces around *username.*

```
> show running-config | grep {{username}}
```

You can name your parameters anything you want. You can also create the same macro with this parameter name:

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

The parameter name can be descriptive and must use alphanumeric characters and underlines. The command syntax, in this case the

```
show running-config | grep
```

part of the command, must use proper CLI syntax for the device you are sending the command to.

Create a CLI Macro from a New Command

Procedure

Step 1 Before you create a CLI macro, test the command in Security Cloud Control's Command Line Interface to make sure the command syntax is correct and it returns reliable results.

Note
- For detailed ASA CLI documentation, see ASA Command Line Interface Documentation, on page 87.

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

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

Step 4 Click the appropriate device type tab and select an online and synced device.

Step 5 Click **>_Command Line Interface.**

Step 6 Click the CLI macro favorites star to see what macros already exist.

Step 7 Click the the plus button.

Step 8 Give the macro a unique name. Provide a description and notes for the CLI macro if you wish.

Step 9 Enter the full command in the **Command** field.

Step 10 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 11 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a CLI Macro.

Create a CLI Macro from CLI History or from an Existing CLI Macro

In this procedure, you are going to create a user-defined macro from a command you have already run, another user-defined macro, or from a system-defined macro.

Procedure

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

Note If you want to create a user-defined macro from CLI history, select the device on which you ran the command. CLI macros are shared across devices on the same account but not CLI history.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select an online and synced device.

Step 4 Click **>_Command Line Interface.**

Step 5 Find the command you want to make a CLI macro from and select it. Use one of these methods:

- Click the clock to view the commands you have run on that device. Select the one you want to turn into a macro and the command appears in the command pane.
- Click the CLI macro favorites star to see what macros already exist. Select the user-defined or system-defined CLI macro you want to change. The command appears in the command pane.

Step 6 With the command in the command pane, click the CLI macro gold star . The command is now the basis for a new CLI macro.

Step 7 Give the macro a unique name. Provide a description and notes for the CLI macro if you wish.

Step 8 Review the command in the Command field and make the changes you want.

Step 9 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 10 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a CLI Macro.

Run a CLI Macro

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select one or more devices.

Step 4 Click **>_Command Line Interface.**

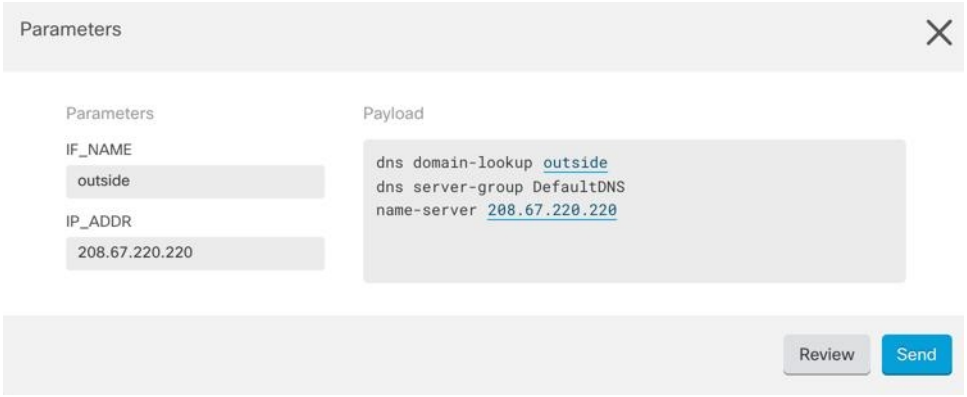
Step 5 In the command panel, click the star .

Step 6 Select a CLI macro from the command panel.

Step 7 Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Configure DNS macro below, click **>_ View Parameters.**

Step 8 In the Parameters pane, fill in the values for the parameters in the Parameters fields.



Step 9 Click **Send**. After Security Cloud Control has successfully, sent the command and updated the device's configuration, you receive the message, Done!

- For an ASA the running configuration is updated.

Step 10 After you send the command you may see the message, "Some commands may have made changes to the running config" along with two links.

- Clicking **Write to Disk** saves the changes made by this command, and any other change that in the running config, to the device's startup config.
- Clicking **Dismiss**, dismisses the message.

Edit a CLI Macro

You can edit user-defined CLI macros but not system-defined macros. Editing a CLI macro changes it for all your ASA devices. Macros are not specific to a particular device.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select your device.
Step 5 Click **Command Line Interface**.
Step 6 Select the user-defined macro you want to edit.
Step 7 Click the edit icon in the macro label.
Step 8 Edit the CLI macro in the Edit Macro dialog box.
Step 9 Click **Save**.

See Run a CLI Macro for instructions on how to run the CLI macro.

Delete a CLI Macro

You can delete user-defined CLI macros but not system-defined macros. Deleting a CLI macro deletes it for all your devices. Macros are not specific to a particular device.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select your device.
Step 5 Click >_**Command Line Interface**.
Step 6 Select the user-defined CLI macro you want to delete.
Step 7 Click the trash can icon in the CLI macro label.
Step 8 Confirm you want to remove the CLI macro.

Configure ASA Using Security Cloud Control CLI

You can configure an ASA device by running the CLI commands in the CLI interface provided in Security Cloud Control. To use the interface, click **Security Devices**, select the device and click **Command Line Interface**. For more information, see Using the Security Cloud Control Command Line Interface.

Add a New Logging Server

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts.

For more information, see the 'Monitoring' section of the 'Logging' chapter in the CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Configure the DNS Server

You need to configure DNS servers so that the ASA can resolve host names to IP addresses. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

For more information, see the 'Basic Settings' chapter of the 'Configure the DNS Server' section in CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Add Static and Default Routes

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing.

For more information, see the 'Static and Default Routes' chapter of CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide.

Configure Interfaces

You can configure the management and data interfaces using CLI commands. For more information, see the 'Basic Interface Configuration' chapter of CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide.

Compare ASA Configurations Using Security Cloud Control

Use this procedure to compare the configurations of two ASAs.

Procedure

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

Step 2 Click the **Devices** tab to locate the ASA device or the **Templates** tab to locate the ASA model device.

Step 3 Click the **ASA** tab.

Step 4 Filter your device list for the devices you want to compare.

Step 5 Select two of your ASAs. Their status does not matter. You are comparing the configurations of the ASAs stored on Security Cloud Control.

Step 6 In the Device Actions pane on the right, click **Compare.**

Step 7 In the Comparing Configurations dialog, click **Next** and **Previous** to skip through the differences, highlighted in blue, in the configuration files.

ASA Bulk CLI Use Cases

The following cases are possible workflows you may experience when using Security Cloud Control's bulk CLI function for ASA devices.

Show all users in the running configuration of an ASA and then delete one of the users

Procedure

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

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

Step 3 Click the **ASA** tab.

Step 4 Search and filter the device list for the devices from which you want to delete the user and **select** them.

Note Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy`, and `write`.

Step 5 Click **>_Command Line Interface** in the details pane. Security Cloud Control lists the devices you chose in the My List pane. If you decide to send the command to fewer devices, uncheck devices in that list.

Step 6 In the command pane, enter `show run | grep user` and click **Send.** All the lines in the running configuration file that contain the string user will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.

Step 7 Click the By Response tab and review the responses to determine which devices have the user that you want to delete.

Step 8 Click the My List tab and select the list of devices from which you want to delete the user.

Step 9 In the command pane, enter the no form of the user command to delete user2 and then click **Send**. For the sake of this example, you are going to delete user2:

```
no user user2 password reallyhardpassword privilege 10
```

Step 10 Look in the history panel for the instance of the `show run | grep user` command, you used to search for the user name. Select that command, look at the list of devices in the Execution list and select **Send**. You should see that the username has been deleted from the devices you specified.

Step 11 If you are satisfied that you have deleted the correct users from the running configuration and that the correct users remain in the running configuration:

a. Select the `no user user2 password reallyhardpassword privilege 10` command from the history pane.

b. Click the **By Device** tab and click **Execute a command on these devices**.

c. In the command pane, click **Clear** to clear the command pane.

d. Enter the command `deploy memory` and click **Send**.

Find all SNMP configurations on selected ASAs

This procedure shows you all the SNMP configuration entries in the running configuration of the ASA.

Procedure

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

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

Step 3 Click the **ASA** tab.

Step 4 Filter and search for the devices on which you want to analyze the SNMP configuration in the running configuration and **select** them.

Note Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, and `dir`.

Step 5 Click **Command Line Interface** in the details pane. The devices you chose are in the My List pane. If you decide to send the command to fewer devices, uncheck devices in the list.

Step 6 In the command pane, enter `show run | grep snmp` and click **Send.** All the lines in the running configuration file that contain the string snmp will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.

Step 7 Review the command output in the response pane.

ASA Command Line Interface Documentation

Security Cloud Control fully supports the ASA command line interface. We provide a terminal-like interface within Security Cloud Control for users to send ASA commands to single devices and multiple devices simultaneously. The ASA command line interface documentation is extensive. Rather than recreating parts of it in the Security Cloud Control documentation, here are pointers to the ASA CLI documentation on Cisco.com.

ASA Command Line Interface Configuration Guides

Starting with ASA version 9.1, the ASA CLI Configuration Guide is broken into three separate books:

- CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide
- CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide
- CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide

You can reach the ASA CLI Configuration Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Configure > Configuration Guides.

A Few Specific ASA Command Line Interface Configuration Guide Sections

Filtering show and more Command Output. You can learn about filtering show command output by using regular expressions in CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide under Filter show and more Command Output.

ASA Command Reference

The ASA Command Reference Guide is an alphabetical listing of all the ASA commands and their options. The ASA command reference is not version specific. It is published in four books:

- Cisco ASA Series Command Reference, A - H Commands
- Cisco ASA Series Command Reference, I - R Commands
- Cisco ASA Series Command Reference, S Commands
- Cisco ASA Series Command Reference, T - Z Commands and IOS Commands for the ASASM

You can reach the ASA Command Reference Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Reference Guides > Command References > ASA Command References.

Export Security Cloud Control CLI Command Results

You can export the results of CLI commands issued to a standalone device, or several devices, to a comma separated value (.csv) file so you can filter and sort the information in it however you like. You can export the CLI results of a single device, or many devices at once. The exported information contains the following:

- Device
- Date
- User
- Command
- Output

Export CLI Command Results

You can export the results of commands you have just executed in the command window to a .csv file:

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select the device or devices so they are highlighted.
Step 5 In the **Device Actions** pane for the device, click >_**Command Line Interface**.
Step 6 In the command line interface pane, enter a command and click **Send** to issue it to the device.
Step 7 To the right of the window of entered commands, click the export icon .
Step 8 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Export the Results of CLI Macros

You can export the results of macros that have been executed in the command window. Use the following procedure to export to a .csv file, the results of CLI macros executed on one or multiple devices:

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the **Device Actions** pane for the device, click >_**Command Line Interface**.

Step 6 In the left pane of the CLI window, select the CLI macro favorites star .

Step 7 Click on the macro command you want to export. Fill in any appropriate parameters and click **Send**.

Step 8 To the right of the window of entered commands, click the export icon .

Step 9 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Export the CLI Command History

Use the following procedure to export the CLI history of one or multiple devices to a .csv file:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the Device Actions pane for the device, click >_**Command Line Interface**.

Step 6 Click the **Clock** icon to expand the history pane if it is not already expanded.

Step 7 To the right of the window of entered commands, click the export icon .

Step 8 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Related Information:

- Security Cloud Control Command Line Interface, on page 73
- Create a CLI Macro from a New Command
- Delete a CLI Macro
- Edit a CLI Macro
- Run a CLI Macro
- ASA Bulk CLI Use Cases
- ASA Command Line Interface Documentation
- Bulk Command Line Interface

Export the CLI Macro List

You can only export macros that have been executed ed in the command window. Use the following procedure to export the CLI macros of one or multiple devices to a .csv file:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the Device Actions pane for the device, click **>_Command Line Interface**.

Step 6 In the left pane of the CLI window, select the CLI macro favorites star .

Step 7 Click on the macro command you want to export. Fill in any appropriate parameters and click **Send**.

Step 8 To the right of the window of entered commands, click the export icon .

Step 9 Give the .csv file a descriptive name and save the file to your local file system.

Restore an ASA Configuration

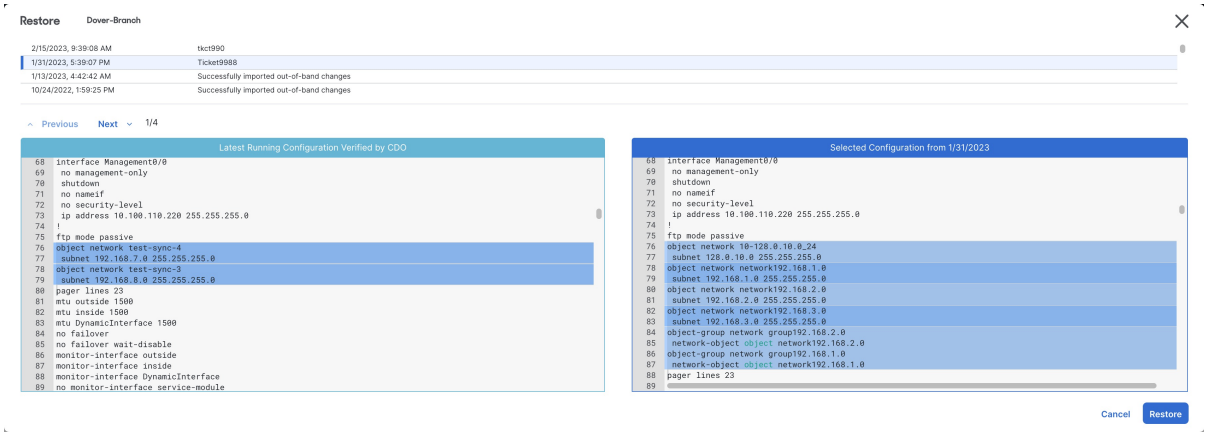
If you make a change to an ASA's configuration, and you want to revert that change, you can restore an ASA's past configuration. This is a convenient way to remove a configuration change that had unexpected or undesired results.

About Restoring an ASA Configuration

Review these notes before restoring a configuration:

- Security Cloud Control compares the configuration you choose to restore with the last known configuration deployed to the ASA, it does not compare the configuration you choose to restore with a configuration that is staged but not deployed to the ASA. If you have any undeployed changes on your ASA and you restore a past configuration, the restore process will overwrite your undeployed changes and you will lose them.
- Before you can restore a past configuration, the ASA can be in a Synced or Not Synced state but if the device is in a Conflict Detected state, the conflict must be resolved before you restore a past configuration.
- Restoring a past configuration overwrites all intermediate deployed configurations changes. For example, restoring the configuration from 1/31/2023 in the list below overwrites the configuration changes made on 2/15/2023.
- Clicking the Next and Previous buttons will move you through the configuration file and highlight the configuration file changes
- If you originally applied a change request label to your configuration changes, that label appears in the Restore Configuration list.

Figure 1: ASA Restore Configuration Screen



How Long are Configuration Changes Kept?

You can restore an ASA configuration that is 1 year old or less. Security Cloud Control restores configuration changes logged in its changelog. The change log records changes every time a configuration change is written to or read from an ASA. Security Cloud Control stores 1 year's worth of changelogs and there is no limitation on the number of the backups made within the previous year.

Restore an ASA Configuration

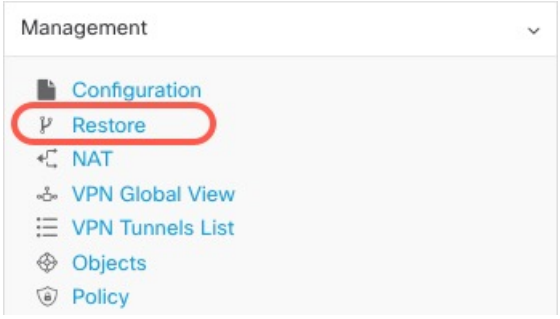
Procedure

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

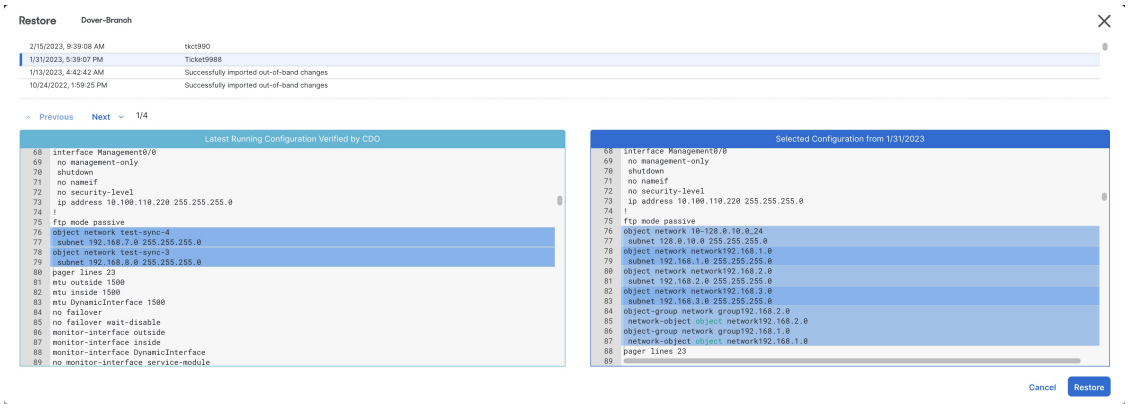
Step 2 Click the ASA tab.

Step 3 Select the ASA whose configuration it is you want to restore.

Step 4 In the **Management** pane, click **Restore.**



Step 5 In the **Restore** page, select the configuration you want to revert to.



For example, in the picture above, the configuration from 1/31/2023 is selected.

Step 6 Compare the "Latest Running Configuration Verified by Security Cloud Control" and the "Selected Configuration from <*date*>" to ensure you want to restore the configuration displayed in the Selected Configuration from <*date*> window. Use the Previous and Next to compare all the changes.

Step 7 Click **Restore,** this stages the configuration in Security Cloud Control. In the **Security Devices** page, you see that the configuration status of the device is now "Not Synced."

Step 8 Click **Deploy Changes...** in the right-hand pane to deploy the changes and sync the ASA.

Troubleshooting

How do I recover changes I lost but wanted to keep?

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the ASA tab.

Step 4 Select the required device.

Step 5 Click **Change Log** in the right pane.

Step 6 Review the changes in the change log. You may be able to reconstruct your lost configurations from those records.

Manage ASA and Cisco IOS Device Configuration Files

Some types of devices such as the ASA and Cisco IOS devices store their configurations in a single file. For these devices, you can view the configuration file on Security Cloud Control and perform a variety of operations on it.

View a Device's Configuration File

For the devices which store their entire configurations in a single configuration file, such as ASA, SSH-managed devices, and devices running Cisco IOS, you can view the configuration file using Security Cloud Control.

Note SSH-managed devices and Cisco IOS Devices have read-only configurations.

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or model whose configuration it is you want to view.

Step 5 In the **Management** pane on the right, click **Configuration**.
The full configuration file is displayed.

Related Information:

- Edit a Complete Device Configuration File

Edit a Complete Device Configuration File

Some types of devices store their configurations in a single configuration file, such as ASA . For these devices, you can view the device configuration file on Security Cloud Control and perform a variety of operations on it depending on the device.

Currently, only ASA configuration files can be edited directly using Security Cloud Control.

Caution This procedure is for advanced users who are familiar with the syntax of the device's configuration file. This method makes changes directly to copy of the configuration file stored on Security Cloud Control.

Procedure

Procedure

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **ASA** tab.

Step 4 Select the device whose configuration it is you want to edit.

Step 5 In the **Management** pane on the right, click **Configuration**.

Step 6 In the **Device Configuration** page, click **Edit**.

Step 7 Click the editor button on the right and select the **Default** text editor, **Vim**, or **Emacs** text editors.

Step 8 Edit the file and save the changes.

Step 9 Return to the **Security Devices** page and preview and deploy the change.

About Device Configuration Changes

In order to manage a device, Security Cloud Control must have its own copy of the device's configuration stored in its local database. When Security Cloud Control "reads" a configuration from a device it manages, it takes a copy of the device's configuration and saves it. The first time Security Cloud Control reads and saves a copy of a device's configuration is when the device is onboarded. These choices describe reading a configuration for different purposes:

- **Discard Changes**: This action is available when a device's configuration status is "Not Synced." In the Not Synced state, there are changes to the device's configuration pending on Security Cloud Control. This option allows you to undo all pending changes. The pending changes are deleted and Security Cloud Control overwrites its copy of the configuration with copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device's configuration status is Synced. Clicking Checking for Changes directs Security Cloud Control to compare its copy of the device's configuration with the copy of the configuration stored on the device. If there is a difference, Security Cloud Control immediately overwrites its copy of the device's configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, Security Cloud Control checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click Review Conflict allows you to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites Security Cloud Control's copy of a device's configuration with the latest copy of the configuration stored on the device. Security Cloud Control does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

Read All: This is a bulk operation. You can select more than one device, in any state, and click **Read All** to overwrite all the devices' configurations stored on Security Cloud Control with the configurations stored on the devices.

- **Deploy Changes**: As you make changes to a device's configuration, Security Cloud Control saves the changes you make to its own copy of the configuration. Those changes are "pending" on Security Cloud Control until they are deployed to the device. When there are changes to a device's configuration that have not been deployed to the device, the device is in the Not Synced configuration state.

  Pending configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an effect. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device. Deployments can be initiated for a single device or on more than one device simultaneously.

- **Discard All** is an option that is only available after you click **Preview and Deploy...**. After clicking Preview and Deploy, Security Cloud Control shows you a preview of the pending changes in Security Cloud Control. Clicking **Discard All** deletes all pending changes from Security Cloud Control and does not deploy anything to the selected device(s). Unlike "Discard Changes" above, deleting the pending changes is the end of the operation.

Note You can schedule deployments or recurring deployments. See Schedule an Automatic Deployment, on page 103 for more information.

Read All Device Configurations

If a configuration change is made to a device outside of Security Cloud Control, the device's configuration stored on Security Cloud Control and the device's local copy of its configuration are no longer the same. You many want to overwrite Security Cloud Control's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

See About Device Configuration Changes for more information about how Security Cloud Control manages the two copies of the device's configuration.

Here are three configuration statuses where clicking **Read All** will overwrite Security Cloud Control's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**-If conflict detection is enabled, Security Cloud Control polls the devices it manages every 10 minutes for changes made to their configurations. If Security Cloud Control finds that the configuration on the device has changed, Security Cloud Control displays a "Conflict detected" configuration status for the device.
- **Synced**-If the device is in a synced state, and you click **Read All**, Security Cloud Control immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, Security Cloud Control confirms your intent to overwrite its copy of the device's configuration and then Security Cloud Control performs the overwrite.
- **Not Synced**-If the device is in the Not Synced state, and you click **Read All**, Security Cloud Control warns you that there are pending changes made to to the device's configuration using Security Cloud Control and that proceeding with the Read All operation will delete those changes and then overwrite Security Cloud Control's copy of the configuration with the configuration on the device. This Read All functions like Discard Configuration Changes.

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 (Optional) Create a change request label to identify the results of this bulk action easily in the Change Log.

Step 5 Select the devices whose configurations you want to save Security Cloud Control. Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Click **Read All**.

Step 7 Security Cloud Control warns you if there are configuration changes staged on Security Cloud Control, for any of the devices you selected, and asks if you want to continue with the bulk reading configurations action. Click **Read All** to continue.

Step 8 Look at the notifications tab for the progress of the Read All configurations operation. If you want more information about how individual actions in the bulk operation succeeded or failed, click the blue Review link and you will be directed to the Jobs page.

Step 9 If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Related Information

- About Device Configuration Changes
- Discard Configuration Changes
- Check for Configuration Changes

Read Configuration Changes from an ASA to Security Cloud Control

Why Does Security Cloud Control "Read" ASA Configurations?

In order to manage an ASA, Security Cloud Control must have it's own stored copy of the ASA's running configuration file. The first time Security Cloud Control reads and saves a copy of the device's configuration file is when the device is onboarded. Subsequently, when Security Cloud Control reads a configuration from an ASA, you are opting to either **Check for Changes**, **Accept without Review**, or **Read Configuration**. See About Device Configuration Changes for more information.

Security Cloud Control also needs to read an ASA configuration in these circumstances:

- Deploying configuration changes to the ASA has failed and the device state is not listed or **Not Synced**.
- Onboarding a device has failed and the device state is **No Config**.
- You have made changes to the device configuration outside of Security Cloud Control and the changes have not been polled or detected. THe device state would be either S**ynced** or C**onflict Detected**.

In these cases, Security Cloud Control needs a copy of the last known configuration stored on the device.

Read Configuration Changes on ASA

When prompted to Read Configuration changes on an ASA:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device that Security Cloud Control has recently failed to onboard or the device that Security Cloud Control has failed to deploy a change to.

Step 5 Click **Read Configuration** in the Synced pane at the right. This option overwrites the configuration currently saved to Security Cloud Control.

Preview and Deploy Configuration Changes for All Devices

Security Cloud Control informs you when you have made a configuration change to a device on your tenant, but you have not deployed that change, by displaying an orange dot on the Deploy icon  . The devices affected by these changes show the status "Not Synced" in the Devices and **Services** page. By clicking **Deploy**, you can review which devices have pending changes and deploy the changes to those devices.

Note For every new FDM or FTD network object or group that you create and make changes to, Security Cloud Control creates an entry in this page for all on-premises management centers that are managed by Security Cloud Control.

This deployment method is available for all supported devices.

You can use this deployment method for single configuration changes or wait and deploy multiple changes at once.

Procedure

Step 1 In the top right corner of the screen, click the **Deploy** icon  .

Step 2 Select the devices with changes you want to deploy. If a device has a yellow caution triangle, you can not deploy changes to that device. Hover your mouse over the yellow caution triangle to find out why you can't deploy changes to that device.

Step 3 (Optional) If you want to see more information about a pending change, click the **View Detailed Changelog** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.

Step 4 (Optional) Create a change request to track your changes without leaving the **Devices with Pending Changes** page.

Step 5 Click **Deploy Now** to deploy the changes immediately to the devices you selected. You'll see the progress in the Active jobs indicator in the Jobs tray.

Step 6 (Optional) After the deployment has finished, click **Jobs** in the Security Cloud Control navigation bar. You will see a recent "Deploy Changes" job showing the results of the deployment.

Step 7 If you created a change request label, and you have no more configuration changes to associate with it, clear it.

What to do next

- About Scheduled Automatic Deployments
- Deploy Configuration Changes from Security Cloud Control to ASA, on page 98
- Change Log Entries after Deploying to an ASA

Deploy Configuration Changes from Security Cloud Control to ASA

Why Does Security Cloud Control Deploy Changes to an ASA?

As you manage and make changes to a device's configuration with Security Cloud Control, Security Cloud Control saves the changes you make to its own copy of the configuration file. Those changes are considered "staged" on Security Cloud Control until they are "deployed" to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control "deploys" the changes to the device do they have an effect on the traffic running through the device. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device.

The ASA has a "running" configuration file, sometimes called the "running config" and a "startup" configuration file that is sometimes called the "startup config." The configuration stored in the running config file is enforced on traffic passing through the ASA. After you make changes to the running config and you are happy with the behavior those changes produce, you can deploy them to the startup config. If the ASA is ever rebooted, it uses the startup config as its configuration starting point. Any changes you make to the running config that are not saved to the startup config are lost after an ASA is rebooted.

When you deploy changes from Security Cloud Control to an ASA, you are writing those changes into the running configuration file. After you are satisfied with the behavior those changes produce, you can deploy those changes to the startup configuration file.

Deployments can be initiated for a single device or on more than one device simultaneously. You can schedule individual deployments or recurring deployments for a single device.

Some Changes are Deployed Directly to the ASA

If you use the Security Cloud Control Command Line Interface Command Line Interface Macros interface on Security Cloud Control to make a change to an ASA, those changes are not "staged" on Security Cloud Control. They are deployed directly to the running configuration of the ASA. When you make changes that way, your device remains "synced" with Security Cloud Control.

About Deploying Configuration Changes

This section assumes you are using Security Cloud Control's GUI or editing the Device Configuration page, *not* using Security Cloud Control's CLI interface or CLI macro interface, to make changes to an ASA configuration file.

Updating an ASA configuration is a two-step process.

Procedure

Step 1 Make changes on Security Cloud Control using one of these methods:

- The Security Cloud Control GUI
- The device configuration on the Device Configuration page

Step 2 After you make your changes, return to the **Security Devices** page and then **Preview and Deploy...** the change to the device.

What to do next

When Security Cloud Control updates an ASA's running configuration with the one staged on Security Cloud Control, or when it changes the configuration on Security Cloud Control with the running configuration stored on the ASA, it attempts to change only the relevant lines of the configuration file if that aspect of the configuration can be managed by the Security Cloud Control GUI. If the desired configuration change **cannot** be made using the Security Cloud Control GUI, Security Cloud Control attempts to overwrite the entire configuration file to make the change.

Here are two examples:

- You **can** create or change a network object using the Security Cloud Control GUI. If Security Cloud Control needs to deploy that change to an ASA's configuration, it would overwrite the relevant lines of the running configuration file on the ASA when the change occurs.
- You **cannot** create a new local ASA user using the Security Cloud Control GUI but you can create one by editing the ASA's configuration on the Device Configuration page. If you add a user on the Device Configuration page, and you deploy that change to the ASA, Security Cloud Control will try to save that change to the ASA's running configuration file by overwriting the entire running configuration file.

Deploy Configuration Changes Made Using the Security Cloud Control GUI

Procedure

Step 1 After you make a configuration change using the Security Cloud Control GUI and save your change, that change is saved in Security Cloud Control's stored version of the ASA's running configuration file.

Step 2 Return to the device on the **Security Devices** page.

Step 3 Click the Devices tab. You should see that the device is now "Not synced."

Step 4 Deploy the changes using one of these methods:

- Click the **Deploy** icon  at the top-right of the screen. This gives you a chance to review the changes you made to the device before you deploy them. Check the device you made changes to, expand the device to review the changes, click **Deploy Now** to deploy the changes.

Note If you see a yellow warning triangle next to your device on the Devices with Pending Changes screen, you cannot deploy a change to it. Hover your mouse over the warning triangle to learn why you can't deploy changes to the device.

- In the Not Synced pane, click **Preview and Deploy....**
  a. Review the commands that will change the ASA configuration file.
  b. If you are satisfied with the commands, choose a Configuration Recovery Preference.

     Note If you choose "Let me know and I will restore the configuration manually." click **View Manual Synchronization Instructions** before continuing.

  c. Click **Apply Changes to Device**.
  d. Click **OK** to acknowledge the success message.

Schedule Automatic Deployments

You can also configure your tenant to schedule deployments to a single device or all devices with pending changes by Schedule an Automatic Deployment.

Deploy Configuration Changes Using Security Cloud Control's CLI Interface

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device whose configuration you want to change.

Step 5 Click **>_Command Line Interface** in the **Actions** pane.

Step 6 If there are any commands in the command line interface table, click **Clear** to remove them.

Step 7 In the top box of the command line interface table, enter your commands at the command prompt. You can run a single command, several commands in a batch by entering each command on its own line, or entering a section of configuration file as a command. Here are some examples of commands you can enter in the command line interface table:

A single command creating the network object "albany"

```
object network albany
host 209.165.30.2
```

Multiple commands sent together:

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
```

```
object network cambridge
host 209.165.50.2
```

A section of a running configuration file entered as a command:

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

Note Security Cloud Control does not require you to move between EXEC mode, Privileged EXEC mode, and Global Configuration mode. It interprets the command you enter in the proper context.

Step 8 After you have entered your commands, click **Send**. After Security Cloud Control has successfully deployed the changes to the ASA's running config file, you receive the message, Done!

Step 9 After you send the command you may see the message, "Some commands may have made changes to the running config" along with two links.

- Clicking **Deploy to Disk** saves the changes made by this command, and any other change in the running config, to the ASA's startup config.
- Clicking **Dismiss**, dismisses the message.

Deploy Configuration Changes by Editing the Device Configuration

Caution This procedure is for advanced users who are familiar with the syntax of an ASA configuration file. This method makes changes directly to the running configuration file stored on Security Cloud Control.

Procedure

Step 1 **Security Devices**Click the **Devices** tab.

Step 2 Click the appropriate device type tab.

Step 3 Select the device whose configuration you want to change.

Step 4 Click **View Configuration** in the **Actions** pane.

Step 5 Click **Edit**.

Step 6 Make your changes to the running configuration and **Save** them.

Step 7 Return to the **Inventory** page. In the Not Synced pane, click **Preview and Deploy...**

Step 8 In the Device Sync pane review the changes.

Step 9 Click **Replace Configuration** or **Apply Changes to Device** depending on the kind of change it is.

Deploy Configuration Changes for a Shared Object on Multiple Devices

Use this procedure when you are making changes to a policy or object shared by two or more devices. You can change a common policy on however many devices use it.

Procedure

Step 1 Open and edit the Policies page or the Objects page containing the shared object you want to edit.

Step 2 Review the shared device list and confirm that you want to make the changes on all the devices mentioned.

Step 3 Click **Confirm**.

Step 4 Click **Save**.

Step 5 Click the **Deploy** icon and Preview and Deploy Configuration Changes for All Devices.

Bulk Deploy Device Configurations

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select all of the devices for which you have made configuration changes on Security Cloud Control. These devices should show "Not Synced" status.

Step 5 Deploy the changes using one of these methods:

- Click the button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

  Note If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

- Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.

Step 6 (Optional) Click the Jobs icon in the navigation bar to view the results of the bulk deploy.

Related Information:

- Schedule an Automatic Deployment, on page 103

About Scheduled Automatic Deployments

Using Security Cloud Control, you can make configuration changes to one or more of the devices it manages and then schedule the changes to be deployed to those devices at a time that is convenient for you.

You can only schedule deployments if you Enable the Option to Schedule Automatic Deployments in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments. A scheduled deployment deploys all the staged changes saved on Security Cloud Control at the date and time set. You can also view and delete scheduled deployments from the Jobs page.

If there were changes made directly to the device that have not been About Device Configuration Changes to Security Cloud Control, the scheduled deployment will be skipped until that conflict is resolved. The Jobs page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

Caution If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

Note When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

Schedule an Automatic Deployment

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window. Follow this procedure to schedule a one-time or a recurring deployment for a single device:

Note If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one ore more devices.

Step 5 In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.

Step 6 Select when the deployment should occur.

- For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
- For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.

Step 7 Click **Save**.

Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select one or more devices.
Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .

Step 6 Edit the recurrence, date, or time of a scheduled deployment.
Step 7 Click **Save**.

Delete a Scheduled Deployment

Follow this procedure to delete a scheduled deployment:

Note If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select one or more devices.

Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Delete** .

What to do next

- About Device Configuration Changes
- Read All Device Configurations, on page 95
- Deploy Configuration Changes from Security Cloud Control to ASA, on page 98
- Preview and Deploy Configuration Changes for All Devices, on page 97

Check for Configuration Changes

Check for Changes to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on Security Cloud Control. You will see the this option when the device is in the "Synced" state.

To check changes:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device, whose configuration you suspect may have been changed directly on the device.

Step 5 Click **Check for Changes** in the Synced pane on the right.

Step 6 The behavior that follows is slightly different depending on the device:

- For device if there has been a change to the device's configuration, you will receive the message:

```
Reading the policy from the device. If there are active deployments on the device, reading will
start after they are finished.
```

  - Click **OK** to continue. The configuration on the device will overwrite the stored configuration on Security Cloud Control.
  - Click **Cancel** to cancel the action.

- For ASA device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on Security Cloud Control. The configuration labeled **Found on Device** is the configuration saved on the ASA.

b. Select either:

1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."

2. **Accept** the out-of-band changes to overwrite the device's configuration stored in Security Cloud Control with the configuration found on the device.

c. Click **Continue**.

Discard Configuration Changes

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using Security Cloud Control. When you click **Discard Changes**, Security Cloud Control *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on Security Cloud Control will be the same as the copy of the configuration on the device and the configuration status in Security Cloud Control will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you have been making configuration changes to.

Step 5 Click **Discard Changes** in the **Not Synced** pane on the right.

- For FDM-managed devices-Security Cloud Control warns you that "Pending changes on Security Cloud Control will be discarded and the Security Cloud Control configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-Security Cloud Control deletes the change immediately.
- For AWS devices-Security Cloud Control displays what you are about to delete. Click **Accept** or **Cancel**.

Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using Security Cloud Control. These changes may be made using the device's command-line interface over an SSH connection or by using a local manager like the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Premises Firewall Management Center on the On-Premises Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

Detecting Out-of-Band Changes on Devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Premises Firewall Management Center, Security Cloud Control checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of Security Cloud Control.

If Security Cloud Control finds that there are changes to the device's configuration that are not stored on Security Cloud Control, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Security Cloud Control detects a conflict, one of two conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to Security Cloud Control's database.
- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.
- In the case of an On-Premises Firewall Management Center, there may be changes made, for instance, to objects outside Security Cloud Control, which are pending to be synchronized with Security Cloud Control or changes made in Security Cloud Control which are pending to be deployed to the On-Premises Firewall Management Center.

Synchronizing Configurations Between Security Cloud Control and Device

About Configuration Conflicts

In the **Security Devices** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Premises Firewall Management Center that you manage using Security Cloud Control, navigate **Tools & Services** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Security Cloud Control) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device. Deploying your changes from Security Cloud Control to the device changes the configuration on the device to match Security Cloud Control's version.
- Changes made to devices outside of Security Cloud Control are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on Security Cloud Control to match the configuration on the device.

Conflict Detection

When conflict detection is enabled, Security Cloud Control polls the device for the default interval to to determine if a change has been made to the device's configuration outside of Security Cloud Control. If Security Cloud Control detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of Security Cloud Control are called "out-of-band" changes.

In the case of an On-Premises Firewall Management Center that is managed by Security Cloud Control, if there are changes that are staged and the device is in **Not Synced** state, Security Cloud Control stops polling the device to check for changes. When there are changes made outside Security Cloud Control which are pending to be synchronized with Security Cloud Control and changes made in Security Cloud Control which are pending to be deployed to the on-premises management center, Security Cloud Control declares the on-premises management center to be in the **Conflict Detected** state.

Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule Polling for Device Changes, on page 111 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Security Cloud Control.

Procedure

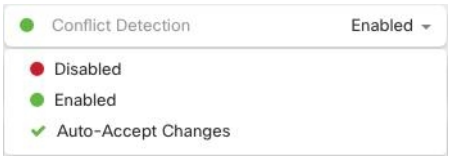
Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Select the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



Automatically Accept Out-of-Band Changes from your Device

You can configure Security Cloud Control to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using Security Cloud Control are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

The auto-accept changes feature is an enhancement to conflict detection. If you have auto-accept changes enabled on your device, Security Cloud Control checks for changes every 10 minutes to determine if there have been any out-of-band changes made to the device's configuration. If there have been configuration changes, Security Cloud Control automatically updates its local version of the device's configuration without prompting you.

Security Cloud Control will ***not*** automatically accept a configuration change if there are configuration changes made on Security Cloud Control that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Security Devices** page; then, you enable auto-accept changes for individual devices.

If you want Security Cloud Control to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection, on page 107 instead.

Configure Auto-Accept Changes

Procedure

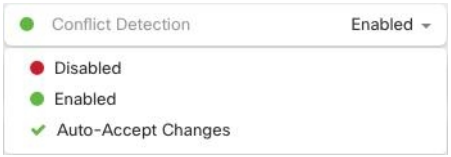
Step 1 Log in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 In the left pane, click **Administration** > **General Settings**.

Step 3 In the **Tenant Settings** area, click the toggle to **Enable the option to auto-accept device changes**. This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Security Devices** page.

Step 4 In the left pane, click **Security Devices** and select the device for which you want to automatically accept out-of-band changes.

Step 5 In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



Disabling Auto-Accept Changes for All Devices on the Tenant

Procedure

Step 1 Log-in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 In left pane, click **Administration** > **General Settings**.

Step 3 In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X. This disables Auto-Accept Changes option in the Conflict Detection menu and disables the feature for every device on your tenant.

Note Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into Security Cloud Control. This includes devices previously configured to auto-accept changes.

Resolve Configuration Conflicts

This section provides information about resolving configuration conflicts that occur on the device.

Resolve the Not Synced Status

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

Procedure

Step 1 In the navigation bar, click **Security Devices**.

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

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reported as Not Synced.

Step 5 In the **Not synced** panel to the right, select either of the following:

- **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

Resolve the Conflict Detected Status

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 107 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

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

Procedure

Step 1 In the navigation bar, click **Security Devices**.

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

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

Step 3 Click the appropriate device type tab.

Step 4 Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.

Step 5 In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

- The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
- The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

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

- **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

  Note As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

Note All configuration changes, rejected or accepted, are recorded in the change log.

Schedule Polling for Device Changes

If you have Conflict Detection, on page 107 enabled, or if you **Enable the option to auto-accept device changes** from the Settings page,Security Cloud Control polls the device for the default interval to determine if a change has been made to the device's configuration outside of Security Cloud Control. You can customize how often Security Cloud Control polls for changes per device. These changes can be applied to more than one device.

If there is no selection configured for a device, the interval is automatically configured for "tenant default".

Note Customizing the interval per device from the **Security Devices** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the Settings page, use the following procedure to schedule how often you want Security Cloud Control to poll your devices:

Procedure

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

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

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the same area as **Conflict Detection**, click the drop-down menu for **Check every** and select the desired polling interval: