



## CHAPTER 5

# Device Management

---

Before you can manage devices in Security Manager, you must prepare the devices so that communication between Security Manager and the devices is enabled, then add those devices to the Security Manager inventory.

This chapter contains the following topics:

- [Troubleshooting Device Communication Failures, page 5-1](#)
- [FAQs About Device Communication, page 5-2](#)
- [Changing Critical Device Properties, page 5-2](#)
- [Security Certificate Rejected When Discovering Device, page 5-6](#)
- [Invalid Certificate Error During Device Discovery, page 5-6](#)
- [Deleting Configuration File When Deleting Security Context, page 5-6](#)
- [Simultaneous Operations on the Same Device, page 5-7](#)
- [Troubleshooting the Setup of CNS-Managed Devices, page 5-7](#)

## Troubleshooting Device Communication Failures

If Security Manager fails to communicate with a device, e.g. by failing to log into it, during discovery, deployment, or other actions, look at these areas to identify and resolve the problem.

- Ensure the device is operational.
- Check the credentials for the device in Security Manager and ensure that they are correct. For existing devices, the credentials are in the Device Properties (right-click the device and select **Device Properties**). When adding new devices the credentials are defined within the New Device wizard if your method of adding the device requires credentials. Keep the following in mind:
  - The primary credentials are used for SSH and Telnet connections.
  - The HTTP/HTTPS credentials are used for HTTP and SSL connections unless you select **Use Primary Credentials**, in which case the primary credentials are also used for these connections.

- Check which transport protocol is selected. You must select a protocol that the device is configured to accept. For most devices, the protocol is selected on the Device Properties General page. For IPS devices, the IPS RDEP mode is selected on the Credentials page.

Some methods of adding devices also allow you to select a non-default transport protocol. To configure the default transport protocols for classes of devices, select **Tools > Security Manager Administration > Device Communications**.

- On the Device Properties General page, ensure that the hostname, domain name, and IP address are correct. Keep in mind that the Hostname and Accounts and Credentials policies for the device define the actual names and credentials that get configured on the device. However, the policies are not used for device communication. If you make changes to the policies that affect the credentials you are using for device communication, you must also manually update the device properties.
- Make sure DNS names can be resolved from the Security Manager server. You might need to fix the DNS settings on the server.

## FAQs About Device Communication

This section answers the following questions about device communication:

- [Q.How does Security Manager connect to a Cisco IOS router that does not have a K8 or K9 crypto image?](#)
  - [Q.Why cannot Security Manager connect to a Cisco IOS router after configuration rollback?](#)
- Q.** How does Security Manager connect to a Cisco IOS router that does not have a K8 or K9 crypto image?
- A.** By default, Security Manager connects to Cisco IOS routers using SSL. However, a device running IOS version 12.3 or later without a K8 or K9 crypto image will not be able to support SSL. Therefore, after you add the device to Security Manager, you must select **Tools > Device Properties**, then change the default transport protocol to Telnet.
- Q.** Why cannot Security Manager connect to a Cisco IOS router after configuration rollback?
- A.** This could occur because of one of the following reasons:
- At rollback, for some versions of Cisco IOS software and when necessary, the configurations are copied from the TFTP server to startup-config, then the Cisco IOS router is reloaded. This reload causes a temporary loss in device connectivity. Wait for the device to be reloaded completely, then try to connect to it again.
  - The configuration contains a nonexistent or unauthorized username and password.

## Changing Critical Device Properties

You must use caution when changing the image version of a device, the device type, or the security context or operational mode of FWSM and ASA devices that are managed by Security Manager. In certain cases, these changes enable a different set of features for the device. As a result, some of the policies that you configured for the device in Security Manager might no longer apply.

The key device changes, their effect on the policies available in Security Manager, and the procedure you should follow to implement these device changes, are described in the following sections:

- [Image Version Changes That Do Not Change the Feature Set in Security Manager, page 5-3](#)
- [Changes That Change the Feature Set in Security Manager, page 5-4](#)

## Image Version Changes That Do Not Change the Feature Set in Security Manager

The following image version changes *do not* affect the types of policies available for that device in Security Manager:

- Upgrading from any Cisco IOS version supported by Security Manager to any other Cisco IOS version supported by Security Manager.
- Upgrading from any PIX 6.x image to another PIX 6.x image.
- Upgrading from any PIX 7.x image to another PIX 7.x image, retaining the same security context and mode configuration.
- Upgrading from any ASA 7.x image to another ASA 7.x image, retaining the same security context and mode configuration.
- Upgrading from any ASA 8.x image to another ASA 8.x image, retaining the same security context and mode configuration.
- Upgrading from any FWSM 2.x image to another 2.x FWSM image, retaining the same security context and mode configuration.
- Upgrading from any FWSM 3.x image to another 3.x FWSM image, retaining the same security context and mode configuration.
- Upgrading a Catalyst 6500/7600 chassis from any IOS 12.x image to another IOS 12.x image.
- Upgrading from IPS 4.x to IPS 5.x or downgrading from IPS 5.x to IPS 4.x.



### Note

This list applies only to images that are supported by Security Manager. For a list of supported images, see *Supported Devices and Software Versions for Cisco Security Manager* for your version of the product at [http://www.cisco.com/en/US/products/ps6498/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html).

In all of these cases, change the image version as follows:

### Procedure

- 
- Step 1** Upgrade the image version on the device.
  - Step 2** Select the device in Security Manager.
  - Step 3** Select **Tools > Device Properties** and update the target OS version property.
  - Step 4** Click **Save**.
-

## Changes That Change the Feature Set in Security Manager

These are the main types of device changes that affect the policy feature set available for a device:

- Image version changes—The following image version changes affect the types of policies available for that device in Security Manager:
  - Upgrading from a PIX 6.x to a PIX 7.x image or from a 7.x to an 8.x image.
  - Downgrading from a PIX 7.x image to a PIX 6.x image or from an 8.x to a 7.x image.
  - Upgrading from an ASA 7.x to an ASA 8.x image.
  - Downgrading from an ASA 8.x to an ASA 7.x image.
  - Upgrading from a FWSM 2.x image to an FWSM 3.x image.
  - Downgrading from a FWSM 3.x image to an FWSM 2.x image.
  - Upgrading from an IOS 12.1 or 12.2 image to an IOS 12.3 or 12.4 image.
  - Downgrading from an IOS 12.3 or 12.4 image to an IOS 12.1 or 12.2 image.

Security Manager prevents you from changing the target OS version of a managed device to a version that changes the types of policies that are available for that device. Therefore, you must first delete the device from Security Manager, perform the image change, then add the device back.

Certain types of policies, such as access rules, are not affected by changes in image version or changes in platform type.

- Security context and operational mode changes—Changes that you make to the security context and operational mode settings on an FWSM or ASA device enable a different set of features on that device. These changes occur if you change the device from:
  - Single context to multiple context (or vice-versa).
  - Routed mode to transparent mode (or vice-versa).

Security Manager prevents you from changing the security context or operational mode settings of a managed device. Therefore, you must first delete the device from Security Manager, change the context or mode, then add the device back.

Certain policy types (for example, Banner, Clock, Console Timeout, and HTTP) are not affected by changes in operational mode. Other policy types (for example, ICMP, SSH, and TFTP, in addition to Banner and Clock) are not affected by changes in security context settings.

- Replacing device hardware—In some cases, you might replace a particular device but retain the original contact information (such as the IP address), for example:
  - Replacing a PIX firewall with a Cisco IOS router
  - Replacing a PIX 7.x device with an ASA device
  - Replacing a Cisco IOS router with a firewall device

In all these cases, the new device changes the types of policies available for that device in Security Manager. Security Manager prevents you from modifying the hardware model of an existing device. Therefore, you must first delete the device from Security Manager, change the physical device, then add the device back.

Certain policy types (for example, access rules) are not affected by changes in device type.

We recommend that you share the policies configured on your device that will not be affected by the change before you remove it from Security Manager. This provides a useful method for reassigning the policies to the device (with any inheritance and policy object references intact) after you add it back to Security Manager.

## Procedure

---

- Step 1** Submit and deploy all the changes you configured for the device in Security Manager. This ensures that the desired configuration is on the device before the image upgrade.
- Step 2** Share the local policies defined on the device:
- Right-click the device in the Device selector, then select **Share Device Policies**. By default, all policies configured on the device (local and shared) are selected for sharing in the Share Policies wizard.
  - Deselect the check box next to each existing shared policy, as indicated by the hand in the policy icon. You should do this because there is no need to create a copy of the shared policies that already exist; you will reassign the existing shared policies after the image version upgrade.
  - Enter a name for the shared policies. We recommend using the device name as a convenient means of identification. For example, if the device name is MyRouter, each shared policy is given the name MyRouter. Make a note of all the policies you are creating for this purpose.
  - Click **Finish**. The selected local policies become shared policies.
- Step 3** Delete the device from Security Manager.
- Step 4** Make the desired change to the device, for example, upgrade the image version, change the operational mode, or replace the device.
- Step 5** Add the device back to Security Manager and perform policy discovery.
- Step 6** Reassign the policies to the device:
- Right-click the first policy type displayed in the Device Policies selector, then select **Assign Shared Policy**.
  - In the Assign Shared Policy dialog box, do one of the following:
    - If a local policy was previously defined on the device, select the shared policy you created for this procedure and click **OK**.
    - If a shared policy of this type was previously assigned to the device, select it and click **OK**.
  - (Local policies only) Right-click the policy type again in the Device Policies selector, then select **Unshare Policy**.
  - Repeat the process for each policy type that is relevant to the device's configuration. If a shared policy is not available, this indicates that this is a policy type that was not available for the previous image version.
- Step 7** (Optional) Delete the shared policies created for this procedure from Policy view:
- Select **View > Policy View** or click the **Policy View** icon on the toolbar.
  - Select one of the policies you want to delete and click the **Assignments** tab in the work area to verify that the policy is not assigned to any devices.
  - Click the **Delete Policy** button beneath the Shared Policy selector to delete the policy.
  - Repeat the process for each policy type that you want to delete.
-

## Security Certificate Rejected When Discovering Device

**Problem** An error occurs when you attempt to discover a device. The error message states that the security certificate received from the device was rejected.

**Solution** Manually enter the thumbprint required by the certificate by doing one of the following:

- Select **Tools > Security Manager Administration > Device Communication**. Click **Add Certificate**, enter the IP address of the device, then copy and paste the thumbprint displayed in the error message into the Certificate Thumbprint field.
- Right-click the device and select **Device Properties > Credentials**. Copy and paste the thumbprint displayed in the error message into the Authentication Certificate Thumbprint field.

You must manually enter the thumbprint whenever you add a new device using the Add New Device or Add From Configuration File options and when you perform rediscovery. It is not required when you add a new device using the Add New Device From Network or Add Device From File options.

## Invalid Certificate Error During Device Discovery

**Problem** If the time settings on the device and Security Manager are not in synchronization, an error message is displayed stating that the certificate is not yet valid when you try to discover a device.

**Solution** When the time set on the Security Manager server is lagging behind the time set on the device, Security Manager cannot validate the device certificate as the start time of the validity period is ahead of the Security Manager time setting. Even if the time zones configured on the device and Security Manager are the same, the invalid certificate error occurs if the daylight saving time (summertime) settings are different. To resolve this problem, make sure that the daylight saving time settings are the same on the device and Security Manager, regardless of whether the time zone is the same. After setting the daylight saving time, synchronize the clock on the device with Security Manager so that both of them display the same time.

To obtain best results, we recommend that you set the same time zone on the device and Security Manager, and modify the time zone after you discover the certificates at a later time, if necessary.

## Deleting Configuration File When Deleting Security Context

**Problem** Deleting a security context from an FWSM device in Security Manager removes the security context from the running configuration of the device, but it does not delete the associated configuration file. This can create problems if you later add another security context with the same name as the one that you previously deleted.

**Solution** This is a known issue for this type of device (as described in CSCsg20999) and is not connected to the behavior of Security Manager. The current workaround is to use the CLI to delete the configuration file from the device.

# Simultaneous Operations on the Same Device

**Problem** Simultaneous operations performed on the same device (that is, devices with the same IP address) produce inconsistent results. For example, deployment to the first device succeeds, but deployment to the second device fails. These simultaneous operations may be a combination of jobs executed by Security Manager, such as a deployment job, and user-initiated operations, such as discovering a live device. Problems can occur whether the operations are contained in the same job or in multiple jobs that are executed at the same time.

**Solution** The device locking mechanism in Security Manager is based on the device name, not the IP address. As a result, operations such as discovery and deployment can run into problems if two devices share the same IP address. This is especially true if you attempt one of these operations on both devices at the same time.

For example, if a deployment job contains two devices with the same IP address, deployment will be executed to both devices because the names are different. However, doing so is not recommended, as it might result in an incomplete or failed deployment. To ensure consistent results, we recommend against defining more than one device with the same IP address.

## Troubleshooting the Setup of CNS-Managed Devices

The following topics describe issues that might arise when you set up a device managed by a Cisco Networking Services (CNS) server and how to solve them:

- [Q. Why do I receive an InvalidParameterException when I click on an IOS device on the CNS web page?](#)
  - [Q. Why am I getting the following error:  
com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: \[002-01003\]\]deviceName does not exists?](#)
  - [Q. Why am I getting the following error:  
com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: \[002-01003\]\]Device device id is not connected](#)
  - [Q. Why is deployment to my CNS-managed PIX device not working?](#)
  - [Q. Why was I able to deploy successfully to a CNS-managed PIX device the first time, but subsequent deployments were unsuccessful?](#)
  - [Q. How do I debug CNS on a PIX device?](#)
  - [Q. How do I debug CNS on an IOS device?](#)
  - [Q. Why did I fail to discover an IOS device and acquire its configuration through CNS?](#)
  - [Q. Why does not the event mode router appear on the CNS Discover Device page or appear in green on the CNS web page?](#)
- Q.** Why do I receive an InvalidParameterException when I click on an IOS device on the CNS web page?
- A.** This is the expected behavior. For IOS devices, Security Manager uses deployment jobs to deploy configurations to CNS 1.5 and 2.0, instead of associating a configuration to the IOS device in CNS. Therefore, you do not see an associated configuration when you click the device name on the CNS web page. For PIX devices, Security Manager associates the configuration to the device in CNS. Therefore, clicking the device name displays the associated configuration.

- Q.** Why am I getting the following error: `com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: [002-01003]]deviceName does not exists?`
- A.** This error indicates that the device has not been added to CNS. It appears if you have not performed rollback or deployment in Security Manager (both of which add the device automatically), and have not manually added the device to CNS.
- Q.** Why am I getting the following error:  
`com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: [002-01003]]Device device id is not connected`
- A.** The answer depends on the type of setup you are performing:
- Event mode setup—Make sure that the CNS device ID defined in the Device Properties window in Security Manager matches the CNS device ID configured on the router (using the **cns id string** command).
  - Call home mode setup—The device is not connected to CNS in this mode; therefore, all Security Manager operations that require the retrieval of the device configuration using CNS are not supported. This includes discovery, preview configuration, display running config, and connectivity tests (and rollback, for IOS devices).
- Q.** Why is deployment to my CNS-managed PIX device not working?
- A.** There are several possibilities:
- The configuration contains invalid commands. You can test this by copying the configuration associated with the PIX device in CNS and pasting it directly into the device.
  - The **auto-update server** command contains an invalid username and password.
  - You did not wait long enough for the configuration to be polled into the PIX device. Use the **show auto** command to verify when the next polling cycle will occur.
  - If you previously used the CNS server for the same PIX device and did not delete the PIX from the CNS server before you started the current task, it is possible that the PIX device received the previous configuration from the CNS server before you deployed the new configuration to it.
  - If none of the suggestions above solves the problem, turn on CNS debug mode (see [Q.How do I debug CNS on a PIX device?](#)) on the PIX device and check the log for errors after the next polling cycle.
- Q.** Why was I able to deploy successfully to a CNS-managed PIX device the first time, but subsequent deployments were unsuccessful?
- A.** This can happen if the configuration pushed during the first deployment contains incorrect CLI commands for the auto-update feature. Check the following:
- Make sure the username and password of the CNS server is defined correctly in the **auto-update** command.
  - Make sure that you have defined a FlexConfig that contains the necessary **name** commands. A FlexConfig is necessary because Security Manager does not support this command directly. As a result, even though the command was discovered, it does not appear in the full configuration.




---

**Note** For more information, see TAC case [CSCsa73337](#).

---

**Q.** How do I debug CNS on a PIX device?

**A.** Enter the following CLI commands:

```
logging monitor debug
terminal monitor
logging on
```



---

**Tip** You can also find relevant information in the PIX log on the CNS server.

---

**Q.** How do I debug CNS on an IOS device?

**A.** Enter the following CLI commands:

```
debug cns all
debug kron exec-cli
terminal monitor
```



---

**Tip** When working in event mode, you can also find relevant information in the event log on the CNS server. When working in call home mode, check the config server log on the CNS server.

---

**Q.** Why did I fail to discover an IOS device and acquire its configuration through CNS?

**A.** If you see the following errors in debug mode:

```
*Feb 23 21:42:15.677: CNS exec decode: Unknown hostname cnsServer-lnx.cisco.com ...
474F6860: 72726F72 2D6D6573 73616765 3E584D4C error-message>XML 474F6870: 5F504152
53455F45 52524F52 3C2F6572 _PARSE_ERROR</er
```

Verify the following:

- The CNS commands use a fully-qualified host name (host name and domain name).
- The device contains **ip domain name** *your domain name*.
- The device contains **ip host** *fully-qualified-cns-hostname cns-ip-address*.

**Q.** Why does not the event mode router appear on the CNS Discover Device page or appear in green on the CNS web page?

**A.** Check the following:

- Make sure that the router and the CNS server can ping each other.
- Clear the **cns event** command, then re-enter it without specifying a port number.

