



# CHAPTER 12

## Deployment

---

This chapter contains the following topics:

- [FAQs About Deployment, page 12-1](#)
- [Changing How Security Manager Responds to Device Messages, page 12-8](#)
- [Performing Rollback When Deploying to a File, page 12-9](#)
- [Mixing Deployment Methods, page 12-9](#)
- [SSL Handshake Failure When Deploying to PIX/ASA Devices, page 12-10](#)
- [Deployment Failures to Devices Managed by AUS, page 12-10](#)

## FAQs About Deployment

This section answers the following questions about deployment:

- [Q.How does Security Manager perform deployment?](#)
- [Q.Which deployment method should I use?](#)
- [Q.How can I control the location used when I deploy to configuration files?](#)
- [Q.If I deploy to files, how does Security Manager know that I applied the configuration to the device?](#)
- [Q.What happens during configuration rollback?](#)
- [Q.After configurations are deployed, which are completely owned by Security Manager, and which are only partially owned, and what does this mean?](#)
- [Q.What happens if I make changes to a device configuration outside of Security Manager \(an out-of-band change\)?](#)
- [Q.What happens during deployment if the version of the OS running on the device is not the same version listed for the device in Security Manager?](#)
- [Q.Can I use Security Manager and ACL Manager together to manage ACLs?](#)
- [Q.Does Security Manager deploy full configurations or only the changes made since the last deployment \(delta configurations\)?](#)
- [Q.What are the default deployment methods for each type of device, and how do I change one for a device or for a deployment job?](#)
- [Q.How many devices can Security Manager deploy to simultaneously?](#)

- Q. Deployment to a Cisco IOS router fails and an “Error Writing to Server” or “Http Response Code 500” error message occurs. Why?
  - Q. Why does deployment to FWSM fail when the configuration contains a large number of ACLs?
  - Q. Why does deployment fail even though the warning expression in the properties files is set to ignore the error?
  - Q. Why do some platforms require a reload after performing configuration rollback but not others?
- Q.** How does Security Manager perform deployment?
- A.** Security Manager performs a three-step process when deploying your configurations to devices, as described in [Table 12-1](#).

**Table 12-1**      **Deployment Process**

<b>Deployment Steps</b>	
<b>Step 1</b>	<p>Security Manager obtains the current configuration for the device and compares it to the most recent saved policies for the device in Security Manager. What Security Manager considers the “current configuration” depends on the type of device, the deployment method, and the settings for deployment preferences. These are the possible sources of configurations and the conditions under which they are used:</p> <ul style="list-style-type: none"> <li>• Obtain the running configuration from the device. <ul style="list-style-type: none"> <li>– Used when deploying to the device <i>unless</i> the deployment method is AUS, TMS, or CNS. You can force Security Manager to use Configuration Archive by selecting Deploy to Device Reference Configuration: Config Archive as the deployment preference (select <b>Tools &gt; Security Manager Administration</b>, then select <b>Deployment</b>).</li> </ul> </li> <li>• Obtain the last full configuration from the Security Manager Configuration Archive. <ul style="list-style-type: none"> <li>– Used when deploying to file, unless you select <b>Deploy to File Reference Configuration: Device</b> as the deployment preference.</li> <li>– Used when the deployment method is TMS or CNS.</li> <li>– Used when the device is not managed by Security Manager.</li> <li>– Used when you preview configurations.</li> </ul> </li> <li>• Obtain the factory default configuration. <ul style="list-style-type: none"> <li>– Used with PIX or ASA devices if you use the AUS deployment method.</li> <li>– Used when previewing PIX or ASA configurations if you use the AUS deployment method.</li> </ul> </li> </ul>

**Table 12-1** *Deployment Process (continued)***Deployment Steps**

- 
- Step 2** Security Manager builds a delta configuration that contains the commands needed to update the device configuration to make it consistent with the assigned policies. It also builds a full device configuration.
- 
- Step 3** If you are deploying to the device, Security Manager deploys either the delta configuration or the full configuration, depending on which deployment method you use. If you are deploying to a file, Security Manager creates two files: *device\_name\_delta.cfg* for the delta configuration, and *device\_name\_full.cfg* for the full configuration. In both cases, the configurations are also added to Configuration Archive. These are the actions based on deployment method:
- SSL or SSH—Security Manager contacts the device directly and sends the delta configuration to it.
  - Auto Update Server (standalone or running on Configuration Engine) for PIX and ASA devices—Security Manager sends the full configuration to Auto Update Server, where the device retrieves it. The delta configuration is not sent.
  - CNS gateway running on an Auto Update Server (for IOS devices with dynamic IP addresses)—Security Manager contacts the CNS gateway to get the device IP address, then uses SSL to contact the device directly and send it the delta configuration.
  - Configuration Engine for IOS devices—Security Manager sends the delta configuration to Configuration Engine, where the device retrieves it.
  - TMS—Security Manager sends the delta configuration to the TMS server, from which it can be downloaded to an eToken to be loaded onto the device.
- 

**Q.** Which deployment method should I use?

**A.** If you are using Configuration Engine (CNS) or Auto Update Server (AUS), use those deployment methods. You must use one of these for devices that use dynamic IP addresses. Otherwise, for devices with static IP addresses, use SSL for IOS, PIX, ASA, and standalone FWSM devices, and SSH for FWSM with Catalyst 6000 and 7600 router devices. If you are using the Token Management Server (TMS) for some devices, you can also use that method with Security Manager.

**Q.** How can I control the location used when I deploy to configuration files?

**A.** To set a default directory for file deployments, select **Tools > Security Manager Administration**, then select **Deployment**. If you select File for the default deployment method, you also select the default directory. When you create a deployment job, you can change this directory for that job. Note that the file location is in the Security Manager server PC not the Security Manager client PC.

**Q.** If I deploy to files, how does Security Manager know that I applied the configuration to the device?

**A.** Security Manager assumes that the previously deployed configuration was applied to the device no matter which deployment method you use. Later deployments include only the changes you made since the last deployment (the delta). If for some reason the last change was not applied to the device, the new delta configuration does not bring the device configuration up to the one reflected in Security Manager.

- Q.** What happens during configuration rollback?
- A.** When you roll back the configuration on a device, Security Manager redeploys either the last good configuration or the configuration that you selected from the Configuration Archive. In either case, after rollback, the configuration on the device is no longer consistent with the configuration in Security Manager. After rollback, you should rediscover policies on the device to make the device configuration and its configuration in Security Manager consistent. Rollback can be triggered from either the deployment manager or the configuration archive. If it occurs from the deployment manager, it rolls back all devices in the job to their last good configuration. If it occurs from the configuration archive, it rolls back to the configuration you select.
- Q.** After configurations are deployed, which are completely owned by Security Manager, and which are only partially owned, and what does this mean?
- A.** When you manage devices that run the ASA, PIX, or FWSM operating systems, Security Manager controls their configurations; you should make all changes within Security Manager. For devices running IOS software, you have more control. If you do not create policies for a feature in Security Manager, such as routing policies, Security Manager does not control those features on the device. If you do create policies for these features, Security Manager overwrites the settings on the device with the settings you defined in Security Manager. Through administration settings, you can control the types of policies that are available for IOS devices, thereby preventing Security Manager from displaying or changing policies for these features. To see the available features for IOS routers and control whether they are available for management in Security Manager, select **Tools > Security Manager Administration**, then select **Policy Management**. For IOS devices, Security Manager does manage VPN-related policies.
- Q.** What happens if I make changes to a device configuration outside of Security Manager (an out-of-band change)?
- A.** During deployment, if Security Manager determines that the configuration on the device differs from the last deployed configuration, Security Manager overwrites the changes by default. (You can control this behavior using the deployment preferences; select **Tools > Security Manager Administration**, then select **Deployment**, and look for the **When Out of Bound Changes Detected** setting. You can also control this for a specific deployment job by selecting **Edit Deployment Method** for the job.)
- Q.** How can I get out-of-band changes into Security Manager?
- A.** If you make changes to the device configuration outside of Security Manager, you have two choices for bringing those changes into Security Manager:
- You can rediscover policies on the device, in which case all policies for the device become local policies, and any assignments of shared policies to the device are removed.
  - You can make the required changes in Security Manager and deploy them to the device.
- Q.** What happens during deployment if the version of the OS running on the device is not the same version listed for the device in Security Manager?
- A.** In some cases, Security Manager deploys the configuration and issues a warning, but in other cases, Security Manager cannot deploy the configuration. Security Manager deploys the configuration when:
- The device has a newer minor version, for example, PIX 6.3(4) instead of the 6.3(1), indicated in Security Manager.
  - Security Manager does not support the version running on the device. In this case, Security Manager builds the configuration using the CLI for the closest supported version.

- The device has a down-level minor version, for example, 6.3(1) instead of 6.3(4).

Security Manager does not deploy the configuration when the device is running a new major version of the OS (for example, PIX 7.0 instead of the 6.3 indicated in Security Manager) or if the device is running a down-level major version (6.3 instead of 7.0).

Table 12-2 lists the possible actions Security Manager takes depending on the whether the OS versions match or differ from each other.



**Note** The PIX Firewall is used as an example; however, the actions apply to all supported device types.

**Table 12-2** Deployment Action Based on OS Version Match or Mismatch

Scenario	OS Version in Security Manager Database	OS Version On Device	OS Version Used In Deployment	Action
Versions match	pix 6.3 (1)	pix 6.3 (1)	pix 6.3 (1)	Deployment proceeds with no warnings.
Device has newer minor OS version.	pix 6.3 (1)	pix 6.3 (4)	pix 6.3 (4)	Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.  Security Manager generates CLI based on the OS version running on the device.
Device has newer minor OS version, which is not supported by Security Manager.	pix 6.3 (1)	pix 6.3 (6)	pix 6.3 (4)	Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.  Security Manager generates CLI based on the highest OS version that it supports.
Device has new major OS version.	pix 6.3 (1)	pix 7.0	pix 7.0	Security Manager reports an error indicating that it has detected a different OS version on the device than the one in the Security Manager database.  Security Manager cannot proceed until you correct this mismatch. Remove the device from inventory and create a new device with the correct OS version.
Device has older OS version.	pix 6.3 (4)	pix 6.3 (1)	pix 6.3 (1)	If the older version is a different major version (6.0 vs. 7.0), Security Manager reports an error and aborts the deployment.  If the older version is within the same major version (6.0 vs. 6.3), Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database, and it continues with the deployment.

- Q.** How do I fix a version mismatch problem?
- A.** You must delete the device, add it again, and discover policies again.

- Q.** Can I use Security Manager and ACL Manager together to manage ACLs?
- A.** Do not use Security Manager and ACL Manager (or any other software) to manage the same ACLs. Use Security Manager to manage all firewall- and VPN-related ACLs. You can use ACL Manager to manage ACLs for other features, such as quality of service (QoS).
- Q.** Does Security Manager deploy full configurations or only the changes made since the last deployment (delta configurations)?
- A.** In most cases, Security Manager sends only delta configurations to the device. The only exception is if you are using Auto Update Server for PIX and ASA devices, in which case the full configuration is sent to the Auto Update Server.
- Q.** What are the default deployment methods for each type of device, and how do I change one for a device or for a deployment job?
- A.** When you add devices to Security Manager, you select the deployment method to be used by that device. This determines the method used for deploying to the device (instead of a file). When you create a deployment job, an additional deployment method default applies to the job as a whole, which determines whether deployment creates configuration files or whether it sends the configuration to the device using the method selected for the device. You control this default in the administration settings (select **Tools > Security Manager Administration**, then select **Deployment**). When you create a deployment job, you can also change whether the deployment is to a file or to the device for each device by clicking **Edit Deploy Method** in the Create Job window.
- Q.** How many devices can Security Manager deploy to simultaneously?
- A.** Security Manager can deploy to up to 20 devices simultaneously per job, up to 40 devices total. These restrictions enable Security Manager to use system memory efficiently, which ensures that jobs with many devices do not prevent jobs with fewer devices from deployment. There is no restriction to the number of jobs that Security Manager processes simultaneously. (You can add as many devices to a deployment job as you desire, there is no limitation. However, Security Manager simultaneously contacts 20 devices per job at most, even though the job has more than 20 devices and up to 40 devices total.)
- Q.** Deployment to a Cisco IOS router fails and an “Error Writing to Server” or “Http Response Code 500” error message occurs. Why?
- A.** When you use SSL as the transport protocol for deploying configurations to a Cisco IOS router, the configuration is split into multiple configuration bulks. The size of this configuration bulk varies from platform to platform. If Security Manager tries to deploy a configuration bulk that exceeds the size of the SSL chunk configured on that device, the deployment fails and you get an “Error Writing to Server” or “Http Response Code 500” error message.

To resolve this, do the following:

1. On the Security Manager server, open the DCS.properties file in the \CSCOPx\MDC\athena\config folder in the installation directory (usually C:\Program Files).
2. Locate **DCS.IOS.ssl.maxChunkSize=<value of the configuration bulk>**.
3. Reduce the value of the configuration bulk.
4. Restart the CiscoWorks Daemon Manager.

- Q.** Why does deployment to FWSM fail when the configuration contains a large number of ACLs?
- A.** This could occur because the CPU utilization is high during ACL compilation. To resolve this, reconfigure the CPU utilization threshold limit by doing the following:
1. On the Security Manager server, open the DCS.properties file in the \CSCOp\MDC\athena\config folder in the installation directory (usually C:\Program Files).
  2. Locate the **DCS.FWSM.checkThreshold=False** property.
  3. Change the value to true: **DCS.FWSM.checkThreshold=True**.
  4. Restart the CiscoWorks Daemon Manager.
  5. Deploy the configuration to the device again.

After you set the value to true, discovery and deployment checks the CPU utilization and generates error messages if the CPU utilization is not within the configured value set in the DCS.FWSM.minThresholdLimit property. The default value is 85.

- Q.** Why does deployment fail even though the warning expression in the properties files is set to ignore the error?
- A.** Setting the properties file to ignore the error is not sufficient. Deployment fails because the Allow Download on Error check box (located on the **Tools > Security Manager Administration > Deployment** page) is deselected by default. To resolve this, select the Allow Download on Error check box and deploy again.

The following tables provide further details about how Security Manager behaves when an error occurs during deployment and the Allow Download on Error checkbox is either selected or deselected:

- [Table 12-3](#) describes the behavior when SSL transport protocol is used on PIX Firewall, ASA, and Cisco IOS routers.
- [Table 12-4](#) describes the behavior when SSH transport protocol is used on Cisco IOS routers.



**Note** On Cisco IOS routers with SSL protocol, deployment on devices stops on command syntax errors. It does not stop when configuration-related errors occur. There is no workaround for this.

**Table 12-3** Security Manager Behavior When SSL is Used on PIX Firewall, ASA, and Cisco IOS Routers

Allow Download on Error	Error Occurred	Error Ignored Using Warning Expression	Deployment Status	Write Memory Done
Selected	Yes	No	Failed	Based on Write Memory flag setting.
Selected	Yes	Yes	Success	Based on Write Memory flag setting.
Selected	No	Not Applicable	Success	Based on Write Memory flag setting.
Deselected	Yes	No	Failed <sup>1</sup>	No
Deselected	Yes	Yes	Failed	No
Deselected	No	Not Applicable	Success	Based on Write Memory flag setting.

1. You get a “Deploy Not Completed” error message.

Table 12-4 Security Manager Behavior When SSH is Used on Cisco IOS Routers

Allow Download on Error	Error Occurred	Error Ignored Using Warning Expression	Deployment Status	Write Memory Done
Selected	Yes	No	Failed	Based on Write Memory flag setting.
Selected	Yes	Yes	Success	Based on Write Memory flag setting.
Selected	No	Not Applicable	Success	Based on Write Memory flag setting.
Deselected	Yes	No	Failed	No
Deselected	Yes	Yes	Success	Based on Write Memory flag setting.
Deselected	No	Not Applicable	Success	Based on Write Memory flag setting.

- Q.** Why do some platforms require a reload after performing configuration rollback but not others?
- A.** On PIX/ASA/FWSM devices, Security Manager uses the replace config option on the device's SSL interface to perform the equivalent of a reload (xlates are cleared, IPsec tunnels are torn down, and so on).

Routers running IOS 12.3(7)T or later use the **configure replace** command to replace the running config with the contents of a configuration file. Support for this command is dependent on the IOS version installed on the router:

- On routers running IOS 12.3(7)T or later, Security Manager copies the configuration file to the startup configuration before executing the **configure replace** command. If the configure replace operation fails, Security Manager issues the **reload** command to reload the operating system using the contents of the startup configuration. Please note that the **reload** command restarts the system, which might result in a temporary network outage.
- On routers running a version prior to 12.3(7)T, Security Manager copies the configuration file to the startup configuration and issues the **reload** command.

## Changing How Security Manager Responds to Device Messages

Security Manager has built-in responses to many of the response messages that can be encountered when configuring a device. You might find that messages Security Manager treats as errors are messages that you want to ignore or treat as informational. Although you can configure your deployment jobs to ignore errors, you might instead want to update Security Manager to treat specific messages differently.

To change how Security Manager treats a message, you need to update the DCS.properties file in \CSCOpX\MDC\athena\config folder in the installation directory (usually c:\Program Files). Use a text editor such as NotePad to update the file.

It is easiest to determine the message you want to ignore by looking at the transcript of a deployment job that encountered the error using these steps:

- 
- Step 1** Select the job with the error message from the Deployment Manager window.
  - Step 2** Click the **Transcript** button in the Deployment Details tab to open the transcript.

- Step 3** Identify the error text that you want to ignore.
- Step 4** Locate the appropriate warning expressions property in the DCS.properties file. For example, for PIX devices the property is called **dev.pix.warningExpressions**, whereas for IOS devices the property is called **dev.ios.warningExpressions**.



**Tip** Conversely, you can make device responses that are not tagged with the Error prefix to appear as error messages. To do this, add the message to the Error Expressions list (for example, **dev.pix.ErrorExpressions**).

- Step 5** Add the error text to the warning expressions list. The warning message should be a generic regular expression string. Except for the last expression, you must delimit all expressions with “\$”. For example, if the message you want to ignore is “Enter a public key as a hexadecimal number,” enter the following string:
- .\*Enter a public key as a hexadecimal number .\*\$**
- Step 6** Restart the CiscoWorks Daemon Manager.

## Performing Rollback When Deploying to a File

You cannot perform rollback when deploying to a file instead of a device. To revert to a previously stored configuration, do the following:

- Step 1** Select **Tools > Configuration Archive**.
- Step 2** In the Configuration Archive window, select a device, then select the configuration to which you want to revert.
- Step 3** Click **View**.
- Step 4** In the Configuration Version Viewer window, make sure the Config Type is set to Full.
- Step 5** Click in the left-hand pane, then press **Ctrl-A** followed by **Ctrl-C** to copy the selected configuration to the Windows clipboard.
- Step 6** Open a text editor, then press **Ctrl-V** to paste the contents of the clipboard.
- Step 7** Save the file. You can then use this file to perform manual rollback.

## Mixing Deployment Methods

**Problem** You receive unpredictable results when you deploy router platform and VPN policies to a live device after previously deploying to a configuration file.

**Solution** This problem can occur when you use a mix of deployment methods (deploy to device and deploy to file) with router platform policies and VPN policies. Because Security Manager does not manage all the available CLI commands for these policy types, it maintains a snapshot of the commands it has configured and leaves all other commands (which includes unsupported commands as well as supported commands in policies that have not been configured in Security Manager) intact on the device.

After each deployment, Security Manager creates a snapshot of the policies that were deployed to each device. This snapshot is used during the next deployment to generate the list of configuration changes that will be deployed to the device. Only one snapshot is maintained at a time per device.

Mixing deployment methods with router platform policies and VPN policies can lead to unpredictable results, as shown in this example:

1. Configure router platform policy A to a live device. When deployment completes, Security Manager creates a snapshot for that device with policy A.
2. Next, configure policy B to replace policy A, but instead of deploying policy B to the device, deploy it to a file instead. When this deployment completes, Security Manager creates a snapshot with policy B that replaces the previous snapshot with policy A. However, because you did not deploy policy B to the device, the CLI commands that are required to negate policy A have not been deployed. Policy A is still deployed on the device.
3. Deploy again to the device without first copying the changes in the configuration file to the device. Security Manager cannot generate the commands that are required to negate policy A from the device because the snapshot with policy A no longer exists.

Because policy A is a router platform policy, any of the following results might occur:

- The policy in the latest deployment overrides policy A.
- Both policies end up defined on the device.
- Deployment fails because the two policies cannot coexist.

Therefore, if you deploy to a file when working on a live device, we strongly recommend that you copy your configuration changes from the file to the device before performing additional deployments to the device.

## SSL Handshake Failure When Deploying to PIX/ASA Devices

**Problem** You receive SSL handshake failures when deploying to PIX or ASA devices.

**Solution** Examine the device's running configuration to verify that the device is using 3DES/AES encryption, not DES. VPN-DES encryption is not supported on Common Services 3.0 and later. If the device is using DES encryption, install a VPN-3DES-AED license and retry deployment.

## Deployment Failures to Devices Managed by AUS

**Problem** Deployment fails when deploying to multiple AUS-managed devices after starting the AUS.

**Solution** This problem can occur if you perform deployment before the Auto Update Server (AUS) is fully operational. The AUS requires time to start up after the following operations:

- New installation or upgrade.
- Manual restart (including after a power outage).
- Manual restart of the Cisco Security Manager Daemon Manager service.

You can verify whether the AUS is fully operational by verifying the status of its Windows services. To do this, select **Start > Control Panel > Administrative Services > Services**, then check the status of the CiscoWorks AUS Database Engine service. If this service has started, try again to deploy.