



CHAPTER 18

Managing Deployment

The settings and policies you define in Security Manager must be deployed to your devices so that you can implement them in your network. The steps you take to deploy configurations to devices depend on whether you are using Workflow mode or non-Workflow mode.

Although non-Workflow mode is the default mode of operation for Security Manager, you can use Workflow mode if your company requires it. For more information, see [Selecting a Workflow Mode, page 2-56](#).

The following topics provide information about deploying configurations to devices, in each workflow mode:

- [Understanding Deployment, page 18-1](#)
- [Working with Deployment, page 18-36](#)

Understanding Deployment

A deployment job defines how configuration changes are sent to devices. In a deployment job, you can define several parameters, such as the devices to which you want to deploy configurations and the method used to deploy configurations to devices. In Workflow mode, you can also specify the dates and times for future deployments.

Understanding these topics will help you better understand and use the deployment feature:

- [Benefits of Deployment Jobs, page 18-2](#)
- [Deployment in Non-Workflow Mode, page 18-3](#)

- [Deployment in Workflow Mode, page 18-5](#)
- [Including Devices in Deployment Jobs, page 18-10](#)
- [Understanding Deployment Methods, page 18-11](#)
- [Deploying to a File, page 18-13](#)
- [Frequently Asked Questions about Deployment, page 18-17](#)

Benefits of Deployment Jobs

The Deployment feature provides these benefits in both Workflow mode and non-Workflow mode, unless noted otherwise:

- **Previewing and comparing configurations**—Before you deploy a configuration file to a device, you can preview the proposed configuration file. You can also compare the proposed configuration file to what was last imported from devices or what is currently running on devices.

After successful deployment to a device, you can view a transcript of the configuration commands downloaded and the device's responses. For more information, see [Previewing Configurations, page 18-43](#).
- **Aborting deployment jobs**—You can stop deployments that have not started to send a configuration file to a device. You cannot stop deployments that are in progress or that have completed. For more information, see [Aborting Deployment Jobs, page 18-47](#).
- **Rolling back to a previous configuration**—If you deploy configurations to devices, and then determine that there is something wrong with the new configurations, you can revert to and deploy the previous configurations for those devices. For more information, see [Rolling Back Configurations to Devices, page 18-48](#).
- **Viewing deployment summary and detailed information**—You can display information about the deployment to specific devices, including information about errors, the proposed configuration, and the transcript of the download. For more information, see [Viewing Deployment Summary Information, page 18-49](#) or [Viewing Deployment Device Details, page 18-50](#).

- Logging deployment job history (Workflow mode only)—You can display the time that a deployment job was created and when configuration files were deployed to devices. You can also track whether the deployment to devices was successful. For more information, see [Viewing Deployment Job History, page 18-57](#).
- Scheduling deployment jobs (Workflow mode only)—You can schedule deployment jobs to occur at future times. This enables you to plan deployments for times when traffic on devices is low. For more information, see [Deployment in Workflow Mode, page 18-5](#).

Deployment in Non-Workflow Mode

These topics help you understand deployment non-Workflow mode:

- [Deployment Task Flow in Non-Workflow Mode, page 18-3](#)
- [Job States in Non-Workflow Mode, page 18-4](#)

Deployment Task Flow in Non-Workflow Mode

The deployment task flow in non-Workflow mode consists of three simple steps (see [Figure 18-1](#)):

1. **Create job:** A deployment job is created for you when you do one of the following:
 - Click the **Submit and Deploy Changes** button on the main toolbar. (Validation is automatically performed on the policies with this option.)
 - Select **File > Deploy**.
 - Select **Tools > Deployment Manager** and click **Deploy**.
2. **Define job:** You specify parameters, such as the devices to which you want to deploy the configurations and whether you want to deploy directly to the devices or to a file.

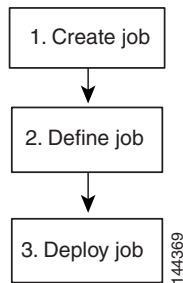
During this step, you can also preview configurations and compare them to the previously deployed configurations or the configuration currently running on the device.



Note Devices selected for one job cannot be included in any other job. This measure ensures that the order policies are deployed is correct.

3. **Deploy job:** Deploying the job sends the generated CLI to devices, either directly or through intermediary transport server (such as AUS, CNS, or TMS) or to output files. The destination (device or file) is selected when defining a job (see step 2). The transport server is selected when defining devices. See [Understanding Deployment Methods, page 18-11](#) for more details about defining deployment methods and transport servers. For information about the affects of deployment on your devices, see [Frequently Asked Questions about Deployment, page 18-17](#).

Figure 18-1 *Deployment Task Flow in Non-Workflow Mode*



Job States in Non-Workflow Mode

In non-Workflow mode, the Status column on the Deployment Manager window lists the state of each job. [Table 18-1](#) lists and describes all possible job states in non-Workflow mode. For more details, see [Deployment Manager Window \(Non-Workflow Mode\)](#), page O-2.

Table 18-1 **Job States in Non-Workflow Mode**

| State | Description |
|--------------|---|
| Deployed | Configurations for all the devices in the job were successfully deployed to the devices or to output files. Devices in the job can now be included in another job. |
| Deploying | Configurations generated for the job are being deployed to the devices or to an output directory (depending on the option selected during job creation). You can monitor the generation progress for specific devices on the Status tab of the Deployment page and on the Job Details page. To access the Job Details page, click the job name in the list. |
| Aborted | Job was manually halted. Devices in the job can now be included in another job. |
| Failed | Deployment to one or more devices in the job failed. Devices in the job can now be included in another job. |
| Rolling Back | Security Manager is in the process of reverting to and deploying previous configurations for the devices within the deployment job. You can abort a job that is in the Rolling Back state. |
| Rolled Back | Security Manager has successfully reverted to and deployed previous configurations for the devices within the deployment job. |

Deployment in Workflow Mode

These topics help you understand deployment in Workflow mode:

- [Deployment Task Flow in Workflow Mode, page 18-5](#)
- [Job States in Workflow Mode, page 18-8](#)
- [Deployment Job Approval, page 18-9](#)
- [Deployment Job Changes, page 18-10](#)
- [Deployment Jobs and Multiple Users, page 18-10](#)

Deployment Task Flow in Workflow Mode

The following is a typical task flow in Workflow mode (see [Figure 18-2](#)):

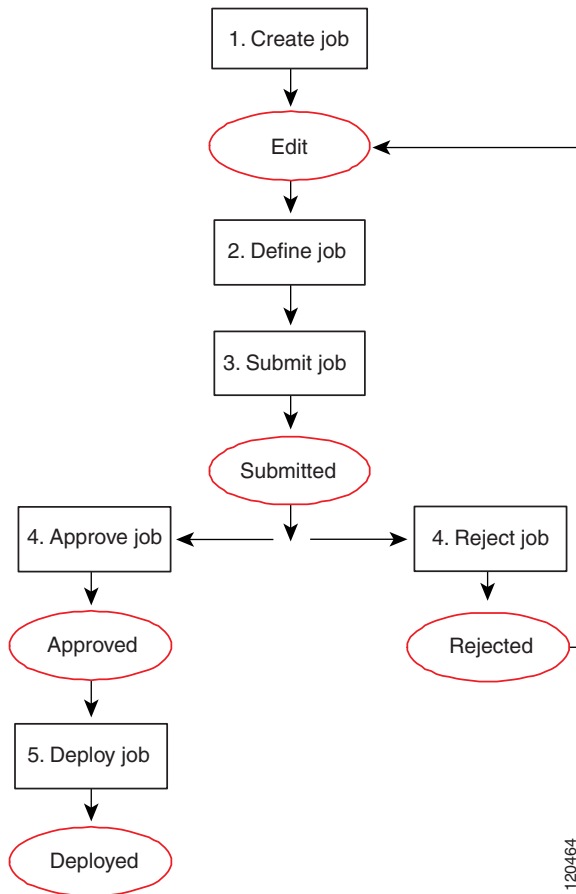
1. **Create job:** Before you deploy configurations to your devices, you must create a deployment job.

2. **Define job:** When you create a job, you specify parameters, such as the devices to which you want to deploy the configurations, whether you want to deploy directly to the devices or to a file, and when you want the job to take place.
3. **Submit job:** If you are using Workflow mode *without* a deployment job approver, you can review and approve the job yourself. Submitting the job submits and approves the job in one step. Proceed to step 6.

In some organizations, before jobs can be deployed, they must be approved by a separate user with the appropriate permissions. In this case, Workflow mode is enabled *with* a deployment job approver, and you must submit the job to this user for review. The user reviews the job and either approves or rejects it.

4. **Approve/Reject job:** If you are working in Workflow mode with a deployment job approver, the approver reviews it, and can then either approve or reject the job. If the job is approved, the submitter can then deploy the job. If the job is rejected, the submitter can discard the job and start over or modify the job and resubmit it.
5. **Deploy job:** Deploying the job sends the generated CLI to either devices, intermediary transport servers (such as AUS, CNS, or TMS), or files. The destination (device or file) is selected when defining a job (see step 2). The transport server is selected when defining devices. See [Understanding Deployment Methods, page 18-11](#) for more details about defining deployment methods and transport servers. For information about the affects of deployment on your devices, see [Frequently Asked Questions about Deployment, page 18-17](#).

For descriptions of job states (shown in red in [Figure 18-2](#)), see [Job States in Workflow Mode, page 18-8](#).

Figure 18-2 *Deployment Task Flow in Workflow Mode*

Job States in Workflow Mode

In Workflow mode, jobs can be in many different states. The Status column in the Deployment Manager window lists the state of each job. [Table 18-2](#) lists and describes all possible job states. For more details about the Deployment Manager window, see [Deployment Manager Window \(Workflow Mode\)](#), page O-10.

Table 18-2 *Job States in Workflow Mode*

| State | Description |
|-------------|---|
| Edit | Job was created, but changes are not being captured in the job. The job can be opened, approved (in auto-approval mode), or discarded while it is in the Edit state. |
| Edit-In Use | Job is open for editing. Changes, such as policy changes, are captured in the job. The job can be closed, approved, discarded, or submitted while it is in the Edit Open state. |
| Submitted | Job was submitted for review. It can be viewed but not edited while it is in the Submitted state. The job can be opened for viewing, discarded, rejected, or approved while it is in the Submitted state. Available only when Workflow mode is enabled with deployment approval required. |
| Approved | Job was approved and is ready to be deployed. The job can be deployed or discarded while it is in the Approved state. Available only when Workflow mode is enabled with deployment approval required. |
| Rejected | Job was rejected. You can open the job for editing or discard the job while it is in the Rejected state. Available only when Workflow mode is enabled with deployment approval required. |
| Discarded | Changes made to the job since the job was created were discarded and further changes to the job are not allowed. The job remains in the Deployment table showing a Discarded state until it is purged from the system. Devices in the job can now be included in another job. |
| Deployed | Configurations for all the devices in the job were successfully deployed to the devices or to output files. Devices in the job can now be included in another job. |
| Deploying | Configurations generated for the job are being deployed to the devices or to an output directory (depending on the option selected during job creation). You can monitor the generation progress for specific devices on the Status tab of the Deployment page and on the Job Details page. To access the Job Details page, click the job name in the list. |
| Aborted | Job was manually halted. Devices in the job can now be included in another job. |

Table 18-2 **Job States in Workflow Mode (continued)**

| State | Description |
|----------------------------|--|
| Failed | Deployment to one or more devices in the job failed. Devices in the job can now be included in another job. |
| Scheduled to run at [date] | Job is scheduled to be deployed at the date and time specified. |
| Rolling Back | Security Manager is in the process of reverting to and deploying previous configurations for the devices within the deployment job. You can abort a job that is in the Rolling Back state. |
| Rolled Back | Security Manager has successfully reverted to and deployed previous configurations for the devices within the deployment job. |

Related Topics

- [Deployment Manager Window \(Workflow Mode\), page O-10](#)
- [Working with Deployment, page 18-36](#)

Deployment Job Approval

By default, Security Manager operates in non-Workflow mode; deployment jobs are handled behind the scenes and the user does not need to be aware of jobs or their approval. When using Workflow mode, you can choose to operate with or without a deployment job approver.

If you choose to operate without an approver, you have the permissions to define and approve jobs.

If your organization requires a different person with higher permissions to approve deployment of new or changed configurations to devices, use Workflow mode with a deployment job approver. When using Workflow mode with a deployment job approver, the job must be reviewed by a person with the appropriate permissions to approve or reject the job. This approval process helps to ensure that no inappropriate configurations reach the network devices and that deployment jobs are scheduled effectively.

**Note**

You enable and disable deployment job approval under Tools > Security Manager Administration > Workflow. For more information, see [Chapter 2, “Performing Administrative Tasks.”](#)

Deployment Job Changes

The changes you make within a deployment job are visible *only* within the deployment job. Other users cannot see your deployment job parameters unless they open your deployment job after you close it.

Deployment Jobs and Multiple Users

Only one user can define or change parameters or devices within an individual deployment job at one time. However, multiple users can work on the same deployment job in sequence: if a deployment job is closed, another user can open it and make changes to it. Multiple users can work in parallel on different deployment jobs.

Including Devices in Deployment Jobs

When you create a job, you select the devices to include in the job. When you select a device for a specific job, it cannot be selected for any other job until the original job is deployed, rejected (Workflow mode), discarded, or aborted. This mechanism prevents two or more people from deploying changes to the same device at the same time and ensures that policies are deployed to devices in the correct order.

When deploying a job, Security Manager displays devices on which policy changes were made but were not deployed. You can deploy to these devices, and you can select additional devices.

For VPNs, Security Manager must generate commands for devices that are affected by the policies defined for the devices you select for the job. So, if you select a device that is part of a VPN, Security Manager adds the other relevant devices to the job. For example, if you define a tunnel policy on a spoke, and you select the spoke for the job, Security Manager adds the spoke’s assigned hub to the job. During job generation, Security Manager generates commands for both

peers so that the VPN configuration is complete and the tunnel can be established. If you deselect one of the devices associated with the VPN, Security Manager warns that removing the device might result in the VPN not functioning properly.

Understanding Deployment Methods

Security Manager uses two types of deployment methods:

- [Deploying to a Device, page 18-11](#) (default)
- [Deploying to a File, page 18-13](#)

If necessary, you can change the default deployment method. For more information, see [Changing Deployment Methods, page 18-44](#).

Deploying to a Device

If you choose to deploy to the device, Security Manager deploys the configuration to the device according to the transport protocol that the device supports and that is configured on the device (see [Table 18-3](#)) and whether a transport server is specified when adding devices (see [Table 18-4](#)).

When deploying directly to a device, Security Manager uploads the device's current configuration and compares it against the configuration it has in its database. If changes were made to the device manually (using the CLI), Security Manager does one of the following, depending on the behavior you define:

- Overwrites change and shows warning.
- Cancels deployment.
- Does not check for changes.

You can set a default behavior under **Tools > Security Manager Administration**. For more information, see [Defining Deployment Settings, page 2-65](#).



Caution

You must configure at least one policy on a device before deploying to that device. If you deploy to a device without assigning at least one policy, the device's current configuration is overwritten with a blank configuration.


Table 18-3 Deployment Transport Protocols

| Device Type | Transport Protocol | Description |
|-------------------------------------|--------------------|--|
| ASA, IOS Router, FWSM, PIX Firewall | SSL (Default) | Security Manager deploys the configuration to the device using a Secure Socket Layer (SSL) protocol. With this protocol, Security Manager encrypts the configuration file and sends it to the device. Note DES encryption is not supported on Common Services 3.0 and later. Please make sure that all PIX Firewalls and Adaptive Security Appliances that you intend to manage with Cisco Security Manager have a 3DES/AES license. |
| Catalyst 6500/7600 | SSH (Default) | Security Manager deploys the configuration to the device using a Secure Shell (SSH). This provides strong authentication and secure communications over insecure channels. Security Manager supports both SSHv1.5 and SSHv2. Once connected to the device, Security Manager determines which version to use and downloads using that version. |

Table 18-4 Deployment Transport Servers

| Device Type | Transport Server | Description |
|-------------------|------------------|---|
| ASA, PIX Firewall | AUS | This option is used to deploy configurations to dynamically addressed devices. Security Manager deploys the configuration file to the Auto Update Server (AUS), where it is stored for later retrieval from the device. Devices, such as PIX Firewalls, that use a Dynamic Host Configuration Protocol (DHCP) server contact AUS for configuration (and image) updates. See AUS Setup Checklist, page 18-30 and the AUS product documentation for more information. |

Table 18-4 Deployment Transport Servers (continued)

| Device Type | Transport Server | Description |
|-------------|------------------|--|
| IOS Routers | CNS | This option is used to deploy configurations to dynamically addressed devices. Security Manager deploys the configuration file to the Cisco Configuration Engine (CE), where it is stored for later retrieval from the device. Devices, such as IOS routers, that use a Dynamic Host Configuration Protocol (DHCP) server contact the CE for configuration (and image) updates. See CNS Setup Checklist, page 18-33 and the CE product documentation for more information. |
| IOS Routers | TMS | Security Manager uses FTP to deploy the configuration file to the Token Management Server (TMS), from which it can be downloaded and encrypted onto an eToken. The eToken can then be connected to the USB port of a router and the configuration downloaded. See TMS Setup Checklist, page 18-28 and the TMS product documentation for more information. |
| | |  <p>Note To deploy using TMS, you must configure token management under Tools > Security Manager Administration > Device Communication > Token Management and configure FTP on the token management server.</p> |

Deploying to a File

You can deploy a configuration to a file on a selected server. If you are deploying to file, Security Manager creates two files: *device_name_delta.cfg* for the delta configuration, and *device_name_full.cfg* for the full configuration. You must specify the directory on the Security Manager server in which to create the configuration files. Configuration files are in TFTP format so that you can upload them to your devices using TFTP.



Note

If you deploy to file, you must transfer the configurations to your devices. Security Manager assumes that you have done this, so the next time you deploy to the same devices, the generated incremental commands are based on the configurations from the previous deployment.

Deploying configurations to a file is useful when the devices are not yet in place in your network (known as greenfield deployment), if you have your own mechanisms in place to transfer configurations to your devices, or if you want to delay deployment.

**Note**

Commands requiring interaction with the device during deployment should not be used when deploying to file. We recommend previewing your configuration before deployment to make sure there are no such commands in the file. For more information, see [Previewing Configurations, page 18-43](#).

Handling Device OS Version Mismatches

Before deploying a changed configuration file to a device, Security Manager uploads the current running configuration file from the device and checks the OS version running on the device with the OS version stored in the Security Manager database. Security Manager takes action depending on whether the OS versions match or differ from each other.

[Table 18-5](#) lists the possible actions Security Manager takes depending on the whether the OS versions match or differ from each other.

**Note**

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

Table 18-5 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 OS version. | pix 6.3 (1) | pix 6.3 (4) | pix 6.3 (4) | <p>Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.</p> <p>Security Manager generates CLI based on the OS version running on the device.</p> |
| Device has newer OS version, which is not supported by Security Manager. | pix 6.3 (1) | pix 6.3 (6) | pix 6.3 (4) | <p>Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.</p> <p>Security Manager generates CLI based on the highest OS version that it supports.</p> |

Table 18-5 *Deployment Action Based on OS Version Match or Mismatch (continued)*

| Scenario | OS Version in Security Manager Database | OS Version On Device | OS Version Used In Deployment | Action |
|----------------------------------|--|-----------------------------|--------------------------------------|--|
| Device has new major OS version. | pix 6.3 (1) | pix 7.0 | pix 7.0 | <p>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.</p> <p>Security Manager cannot proceed until you correct this mismatch. Remove the device from inventory and create a new device with the correct OS version.</p> |

Table 18-5 Deployment Action Based on OS Version Match or Mismatch (continued)

| Scenario | OS Version in Security Manager Database | OS Version On Device | OS Version Used In Deployment | Action |
|------------------------------|---|----------------------|-------------------------------|--|
| Device has older OS version. | pix 6.3 (4) | pix 6.3 (1) | pix 6.3 (1) | <p>If the older version is a different major version (6.0 vs. 7.0), Security Manager reports an error and aborts the deployment.</p> <p>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.</p> |

Frequently Asked Questions about Deployment

These questions and answers describe how policy deployment modifies your device configurations:

1. [How does deployment work?](#)
2. [Which deployment method should I use?](#)
3. [How can I control the location used when I deploy to a configuration file?](#)
4. [If I deploy to file, how does Security Manager know that I applied the configuration to the device?](#)
5. [What happens during configuration rollback?](#)

6. After configurations are deployed, which are completely owned by Security Manager, and which are only partially owned, and what does this mean?
7. What happens if I make changes to a device configuration outside of Security Manager (an out-of-band change)? How can I get the changed configurations into Security Manager?
8. 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? How do I fix a version mismatch problem?
9. How is ACL configuration managed when I use Security Manager and ACL Manager together?
10. Does Security Manager deploy full configurations or only the changes made since the last deployment (delta configurations)?
11. 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?
12. To how many devices can Security Manager deploy simultaneously?
13. Deployment to a Cisco IOS router fails and an “Error Writing to Server” or “Http Response Code 500” error message occurs. Why?
14. Why does deployment to FWSM fail when the configuration contains a large number of ACLs?
15. Why does deployment fail even though the warning expression in the properties files is set to ignore the error?
16. How can I deploy configurations to devices using a Token Management Server (TMS)?
17. How can I deploy configurations to devices using an Auto Update Server (AUS)?
18. How can I deploy configurations to devices using a Cisco Networking Services (CNS) server?
19. Why do some platforms require a reload after performing configuration rollback but not others?

- Q.** How does deployment work?
- A.** Broadly speaking, deployment is a three-step process, as described in [Table 18-6](#).

Table 18-6 Overview of the Deployment Process

Deployment Steps

- Step 1** Security Manager obtains the current configuration for the device and compares it to the latest 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 and the conditions under which they are used:
- Obtain the running configuration from the device.
 - Used when deploying to the device *unless* the deployment method is AUS, TMS, or CNS. You can force Security Manager to use Configuration Archive by selecting **When Deploying to Device Get Reference Config from: Config Archive** as the deployment preference (select **Tools > Security Manager Administration**, then select **Deployment**).
 - Obtain the last full configuration from the Security Manager Configuration Archive.
 - Used when deploying to file, unless you select **When Deploying to File Get Reference Config from: Device** as the deployment preference.
 - Used when the deployment method is TMS or CNS.
 - Used when the device is unmanaged (not managed by Security Manager).
 - Used when deploying to a device if uploading the configuration from the device failed. (Configuration Archive is used as a backup to obtaining the configuration from the live device.)
 - Used when you preview configurations.
 - Use the factory default configuration.
 - Used with PIX or ASA devices if you use the AUS deployment method.
 - Used when previewing PIX or ASA configurations if you use the AUS deployment method.
-

Table 18-6 Overview of the 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 | <p>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 file, Security Manager creates two files: <i>device_name_delta.cfg</i> for the delta configuration, and <i>device_name_full.cfg</i> for the full configuration. In both cases, the configurations are also added to Configuration Archive. These are the actions based on deployment method:</p> <ul style="list-style-type: none"> • 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. <p>Q. Which deployment method should I use?</p> <p>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.</p> |

- Q.** How can I control the location used when I deploy to a configuration file?
- 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.
- Q.** If I deploy to file, 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 will 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. If you roll back configurations on Catalyst or IOS devices, you also need to restart the device.
- 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 will be 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)? How can I get the changed configurations into Security Manager?
- 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 editing the deployment method for the job.) If you make changes to the device configuration outside of Security Manager, you have two choices for bringing those changes into Security Manager:
1. 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.
 2. You can make the required changes in Security Manager and redeploy them to the device. During deployment, do not select the option to force an error if out-of-band changes are found on 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? How do I fix a version mismatch problem?
- 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), even if 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)). If 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), Security Manager cannot deploy the configuration. You must delete the device, add it again, and rediscover policies. Similarly, if the device is running a down-level major version (6.3

instead of 7.0), the deployment fails, and you must re-create the device in Security Manager. See [Handling Device OS Version Mismatches, page 18-14](#).

- Q.** How is ACL configuration managed when I use Security Manager and ACL Manager together?
- 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.** To how many devices can Security Manager deploy 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.

- 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. Go to `...\CSCOPx\MDC\athena\config`.
 2. Select **DCS.properties file** to open the DCS properties file.
 3. Locate **DCS.IOS.ssl.maxChunkSize=<value of the configuration bulk>**.
 4. Reduce the value of the configuration bulk.
 5. 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. Go to `...\CSCOPx\MDC\athena\config`.
 2. Select **DCS.properties file** to open the DCS properties file.
 3. Locate the **DCS.FWSM.checkThreshold=False** property.
 4. Change the value to true: **DCS.FWSM.checkThreshold=True**.
 5. Restart the CiscoWorks Daemon Manager.
 6. 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 18-7](#) describes the behavior when SSL transport protocol is used on PIX Firewall, ASA, and Cisco IOS routers.
- [Table 18-8](#) 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 18-7 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 ¹ | 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 18-8 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 |

Table 18-8 Security Manager Behavior When SSH is Used on Cisco IOS Routers (continued)

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

- Q.** How can I deploy configurations to devices using a Token Management Server (TMS)?
- A.** To perform this type of deployment, you need to set up the device, TMS, and Security Manager. The following checklist shows the tasks that you need to perform.

Table 18-9 TMS Setup Checklist

| ✓ | Task |
|--------------------------|--|
| <input type="checkbox"/> | <p>1. Set up the TMS as an FTP server.</p> <p>You must set up the TMS as an FTP server because files are transferred from Security Manager to the TMS server using FTP.</p> |
| <input type="checkbox"/> | <p>2. Add devices to Security Manager inventory.</p> <p>Select File > Add Devices.</p> |
| <input type="checkbox"/> | <p>3. Specify TMS as the transport protocol to be used for Cisco IOS devices.</p> <p>You can set this parameter globally for all Cisco IOS devices or for a specific device, as follows:</p> <ul style="list-style-type: none"> Globally—Select Tools > Security Manager Administration > Device Communication. Device—Select Device properties > DCS settings > Transport protocols. |
| <input type="checkbox"/> | <p>4. Configure TMS parameters on Security Manager.</p> <p>Specify the TMS name or IP address, username and password, directory where configuration files are to be copied, and public key file information in Security Manager. Select Tools > Security Manager Administration > Token Management.</p> |

Table 18-9 TMS Setup Checklist (continued)

| ✓ | Task |
|---|--|
| ☐ | <p>5. Set the deployment method to Device either globally or for a specific device.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • Globally—Select Tools > Security Manager Administration > Deployment. • Device—Depends on workflow mode: <ul style="list-style-type: none"> – Non-Workflow mode—Select Submit and Deploy Changes > Edit Deploy Method. – Workflow mode—Select Tools > Deployment Management > Create > Edit Deploy Method. |
| ☐ | <p>6. Deploy the configuration to the device.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • Non-Workflow mode—Select Submit and Deploy Changes. • Workflow mode (if no deployment job exists)—Select Tools > Deployment Management > Create. • Workflow mode (if a deployment already job exists)—Select Tools > Deployment Management and select the desired deployment job; then click Deploy. |
| ☐ | <p>7. Using TMS, download the configuration to the eToken.</p> <p>See TMS product documentation.</p> |
| ☐ | <p>8. Download the configuration from the eToken to the router and save the configuration to the device.</p> <p>Plug the eToken into the router, then enter the following commands to download the configuration to the router:</p> <pre>router# crypto pki token <usb_token_id> login <PIN> router# config terminal router(config)# crypto pki token default secondary config CCCD router(config)# exit router# write memory</pre> |

**Tip**

For more information, click **Help** from any Security Manager dialog box or page.

- Q.** How can I deploy configurations to devices using an Auto Update Server (AUS)?
- A.** To perform this type of deployment, you need to set up AUS, the device, and Security Manager. The following checklist shows the tasks that you need to perform.

Table 18-10 **AUS Setup Checklist**

| ✓ | Task |
|--------------------------|---|
| <input type="checkbox"/> | <p>1. Set up the AUS.</p> <p>See the AUS product documentation.</p> |
| <input type="checkbox"/> | <p>2. Bootstrap firewall devices for AUS.</p> <p>Enter the following commands to bootstrap devices:</p> <pre>hostname(config)# auto-update server https://username:password@AUSserver_IP_address:port/autoupdate/AutoUpdateServlet hostname(config)# auto-update poll-period poll_period [retry_count] [retry_period] hostname(config)# auto-update device-id hardware-serial hostname ipaddress [<if_name>] / mac-address [<if_name>] string<text> hostname(config)# write memory</pre> |

Table 18-10 AUS Setup Checklist (continued)

| ✓ | Task |
|---|--|
| ☐ | <p>3. Add devices to Security Manager inventory and assign AUS to devices.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • If you are adding a new device, from the Device view, select File > New Device > Add New Device. Configure the following fields on the Device Information page: <ul style="list-style-type: none"> – Device selector—Select a PIX Firewall or ASA device type. – IP Type—Select Static or Dynamic. – Auto Update Server—Click the arrow to display a list of servers. Select the server that is managing the device. If the server does not appear in the list, click the arrow, then select + Add Server... to add the server. – Device Identity—Enter the string value that uniquely identifies the device in AUS. • If you are adding a device by importing it from DCR, from the Device view, select File > New Device > Add Device From DCR. The device must have been created as an AUS device in DCR for it to be successfully imported into Security Manager as an AUS device. For more information, see Adding Devices to the Security Manager Inventory, page 5-30. |
| ☐ | <p>4. Configure AUS settings in Security Manager.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • (Device view) Select Platform > Device Admin > Server Access > AUS from the Device Policy selector. • (Policy view) Select PIX/ASA/FWSM Platform > Device Admin > Server Access > AUS from the Policy Types selector. Right-click AUS and select New AUS Policy to create a policy, or select an existing policy from the Policies selector. |

Table 18-10 AUS Setup Checklist (continued)

| ✓ | Task |
|---|--|
| ☐ | <p>5. Set the deployment method to Device.</p> <p>You can set this parameter either globally or for a specific device, as follows:</p> <ul style="list-style-type: none"> • Globally—Select Tools > Security Manager Administration > Deployment. • Device—Depends on workflow mode: <ul style="list-style-type: none"> – Non-Workflow mode—Select Submit and Deploy Changes > Edit Deploy Method – Workflow mode—Select Tools > Deployment Management > Create > Edit Deploy Method. |
| ☐ | <p>6. Deploy the configuration to the device.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • Non-Workflow mode—Select Submit and Deploy Changes. • Workflow mode (if no deployment job exists)—Select Tools > Deployment Management > Create. • Workflow mode (if a deployment already job exists)—Select Tools > Deployment Management and select the desired deployment job; then click Deploy. |

Q. How can I deploy configurations to devices using a Cisco Networking Services (CNS) server?

A. To perform this type of deployment, you need to set up the configuration engine (CE), the device, and Security Manager. The following checklist shows the tasks that you need to perform.



Note

If PIX Firewall and ASA devices are configured for CNS, they use the AUS protocol. The required steps are identical to the steps that you follow when you configure PIX Firewall and ASA for AUS. See [How can I deploy configurations to devices using an Auto Update Server \(AUS\)?](#), page 18-30

Table 18-11 CNS Setup Checklist

| ✓ | Task |
|---|---|
| ☐ | <p>1. Set up the Configuration Engine.</p> <p>To set up the Configuration Server on AUS, see the AUS product documentation. To set up the Configuration Server on another server, see the Configuration Server documentation.</p> |
| ☐ | <p>2. Bootstrap devices for CNS.</p> <p>If PIX Firewall and ASA devices are configured for CNS, they use the AUS protocol. The required steps are identical to the steps that you follow when you configure PIX Firewall and ASA for AUS. See Table 18-10. For Cisco IOS routers, you can configure CNS in the event-bus mode or the call-home mode.</p> <p>To configure CNS in event-bus mode, enter the following commands:</p> <pre>hostname(config)# hostname<name> hostname(config)# ip domain-name <your_domain> hostname(config)# cns trusted-server all-agents <ip_address> hostname(config)# cns event <ip_address> [port] hostname(config)# cns config partial <ip_address> hostname(config)# cns password <password> hostname(config)# cns exec hostname(config)# exit hostname# copy running startup</pre> <p>To configure CNS in call-home mode, enter the following commands:</p> <pre>hostname# config terminal hostname(config)# ip domain-name <your_domain> hostname(config)# cns trusted-server all-agents <ip_address> hostname(config)# kron occurrence occurrence-name [user username] {in [[numdays:]numhours:]nummin at hours:min [[month] day-of-month] [day-of-week]} {oneshot recurring} hostname(config-kron-occurrence)# policy-list <list-name> hostname(config-kron-occurrence)# exit hostname(config)# kron policy-list <list-name> hostname(config-kron-policy)# cli cns config retrieve <ip_address> page /cns/JobbedDynaConfig status http://<ip_address>/cns/PostStatus hostname(config-kron-policy)# exit hostname(config)# cns exec hostname(config)# exit hostname# copy running startup</pre> <p>For more information about these commands, see Setting Up CNS, page 5-15.</p> |

Table 18-11 CNS Setup Checklist (continued)

| ✓ | Task |
|---|---|
| ☐ | <p>3. Add devices to Security Manager inventory.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • If you are adding a new device, from the Device view, select File > New Device > Add New Device. Configure the following fields on the Device Information page: <ul style="list-style-type: none"> – IP Type—Select Static or Dynamic, as appropriate. – Device selector—Select a Cisco IOS router (excludes Cisco 7600 series routers). – CNS-Configuration Engine Server—If the device is using static addressing, select a Configuration Engine from the CNS-Configuration Engine Server field. If the desired Configuration Engine does not appear in the list, you can add it now. Click the arrow, then select + Add Configuration Engine.... The Configuration Engine Properties dialog box appears. <p>If the device is using dynamic addressing, select the server that is managing the device (Auto Update Server or Configuration Engine). If the desired server does not appear in the list, click the arrow, then select + Add Server... The Server Properties dialog box appears.</p> • If you are adding a device that already exists in the network, from the Device view, select File > New Device > Add Device From Network. If the device is using dynamic addressing, you must select the Configuration Engine (CNS Gateway) that is managing the device. If the desired Configuration Engine does not appear in the list, click the arrow, then select + Add Auto Update Server... The Auto Update Server Properties dialog box appears. |

Table 18-11 CNS Setup Checklist (continued)

| ✓ | Task |
|---|---|
| ☐ | <p>4. Set the deployment method to Device.</p> <p>You can set this parameter either globally or for a specific device, as follows:</p> <ul style="list-style-type: none"> • Globally—Select Tools > Security Manager Administration > Deployment. • Device—Depends on workflow mode: <ul style="list-style-type: none"> – Non-Workflow mode—Select Submit and Deploy Changes > Edit Deploy Method. – Workflow mode—Select Tools > Deployment Management > Create > Edit Deploy Method. |
| ☐ | <p>5. Deploy the configuration to the device.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> • Non-Workflow mode—Select Submit and Deploy Changes. • Workflow mode (if no deployment job exists)—Select Tools > Deployment Management > Create. • Workflow mode (if a deployment already job exists)—Select Tools > Deployment Management and select the desired deployment job; then click Deploy. |

- 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.

Working with Deployment

The following topics provide information about managing deployment in *both* Workflow and non-Workflow modes:

- [Using the Main Toolbar, page 18-37](#)
- [Viewing Deployment Status Information, page 18-37](#)
- [Deploying Configurations in Non-Workflow Mode, page 18-38](#)
- [Deploying Configurations in Workflow Mode, page 18-41](#)
- [Previewing Configurations, page 18-43](#)
- [Changing Deployment Methods, page 18-44](#)
- [Refreshing Deployment Status Information, page 18-45](#)
- [Redeploying Configurations to Devices, page 18-45](#)
- [Aborting Deployment Jobs, page 18-47](#)

- [Rolling Back Configurations to Devices, page 18-48](#)
- [Viewing Deployment Summary Information, page 18-49](#)
- [Viewing Deployment Device Details, page 18-50](#)

The following are additional topics that apply only to managing deployment in Workflow mode:

- [Creating Deployment Jobs, page 18-51](#)
- [Opening and Closing Deployment Jobs, page 18-54](#)
- [Submitting Deployment Jobs, page 18-55](#)
- [Approving and Rejecting Deployment Jobs, page 18-56](#)
- [Discarding Deployment Jobs, page 18-57](#)
- [Viewing Deployment Job History, page 18-57](#)

Using the Main Toolbar

In non-Workflow mode, you can use the Save & Deploy Changes button to save your policy changes and automatically create a deployment job that deploys them to devices in your network or to output files. See [Deploying Configurations in Non-Workflow Mode, page 18-38](#) for details.

The Deployment Manager window, which you access by clicking the Deployment Manager button on the main toolbar or by selecting **Tools > Deployment Manager**, also enables you to deploy policy changes and discard deployment jobs. However, you can manage more than the current deployment job and perform additional functions. For more information, see [Viewing Deployment Status Information, page 18-37](#).

Viewing Deployment Status Information

To display a list of deployment jobs and their status, select **Tools > Deployment Manager**. The Deployment Manager window appears. From this window, you can perform various functions depending on the Workflow mode in which you are operating. For more information about these functions, see the following topics:

- Non-Workflow Mode
 - [Deploying Configurations in Non-Workflow Mode, page 18-38](#)

- Refreshing Deployment Status Information, page 18-45
- Redeploying Configurations to Devices, page 18-45
- Aborting Deployment Jobs, page 18-47
- Rolling Back Configurations to Devices, page 18-48
- Viewing Deployment Summary Information, page 18-49
- Viewing Deployment Device Details, page 18-50
- Workflow Mode
 - Creating Deployment Jobs, page 18-51
 - Opening and Closing Deployment Jobs, page 18-54
 - Submitting Deployment Jobs, page 18-55
 - Approving and Rejecting Deployment Jobs, page 18-56
 - Discarding Deployment Jobs, page 18-57
 - Redeploying Configurations to Devices, page 18-45
 - Aborting Deployment Jobs, page 18-47
 - Rolling Back Configurations to Devices, page 18-48
 - Viewing Deployment Summary Information, page 18-49
 - Viewing Deployment Device Details, page 18-50
 - Viewing Deployment Job History, page 18-57

Deploying Configurations in Non-Workflow Mode

When you deploy configurations, you can transfer them to devices either directly or to another transport server (such as AUS, CNS, or TMS) in the network or to files in a specified directory.



Caution

You must configure at least one policy on a device before deploying to that device. If you deploy to a device without assigning at least one policy, the device's current configuration is overwritten with a blank configuration.

Notes

- Deployment might take from a few minutes to an hour or more, depending on the number of devices in the deployment job.
- Firewall devices only—If you manually added a firewall device or added a device from DCR, we highly recommend that you discover (import) the factory-default policies for that device before deploying to that device. Bringing these policies into Security Manager prevents you from unintentionally removing them the first time you deploy to that device. For more information about factory-default policies for firewall devices, see [Chapter 15, “Understanding Factory-Default Configurations.”](#) For more information about importing policies, see [Chapter 18, “Managing Deployment.”](#)
- The status of deployments to Catalyst 6500/7600 devices shows deployment to the device as well as its interface contexts when policy changes contain interface commands that affect the interface contexts (child devices). This can occur when you deploy a policy change that affects a VLAN in which the switch participates or when you update inventory, for example, by adding or deleting interface contexts.

Before You Begin

- Make sure that devices have been bootstrapped. For more information, see [Preparing the Devices for Security Manager to Manage, page 5-2.](#)
- If you are deploying to a transport server, such as AUS, CNS, or TMS, make sure the server, Security Manager settings, and device have been set up properly.

Procedure

-
- Step 1** Click the **Submit & Deploy Changes** button on the Main toolbar.
- The Deploy Saved Changes dialog box appears. For a description of the elements in this dialog box, see [Deploy Saved Changes Dialog Box, page O-3.](#)
- Step 2** Select the devices to which you want to deploy configurations.
- Step 3** To change the method used to deploy configurations (default is Device), click **Edit Deploy Method**.
- The Edit Deployment Method dialog box appears. One of the following deployment methods can be specified for each device:

- **Device**—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see [Deploying to a Device, page 18-11](#).
- **File**—Deploys the configuration file to a file on a selected server. If you select File, enter the directory to which you want to deploy the configuration file or click **Browse** to select from a list of available servers in the Destination column. For more information, see [Deploying to a File, page 18-13](#).



Note Before proceeding with the deployment, you can preview proposed configurations and compare them against last deployed configurations or current running configurations. See [Previewing Configurations, page 18-43](#) for more information.

For a description of the elements displayed in the dialog box, see [Edit Deploy Method Dialog Box, page O-17](#).

- Step 4** To add devices that do not have proposed policy changes to the deployment job, click **Add other devices**. You might want to do this if a device was manually modified, and you want to return the device to its previous configuration (the one stored in the Security Manager database).

The Add Devices dialog box appears. Complete the fields in this dialog box. For a description of the elements displayed, see [Add Other Devices Dialog Box, page O-23](#).

- Step 5** Click **Deploy** to deploy the job.

The Deployment Status Details dialog box appears while configurations are being deployed to devices. It displays summary information about the job, status about the deployment to each device, and messages indicating why the deployment failed.

In the Deployment Details table, select a row corresponding to a device to display deployment status messages specifically for that device. For more information, see [Deployment Status Details Dialog Box, page O-6](#).

If deployment to any device failed, you can redeploy configurations to the failed devices. For more information, see [Redeploying Configurations to Devices, page 18-45](#).

Related Topics

- [Including Devices in Deployment Jobs, page 18-10](#)
- [Understanding Deployment Methods, page 18-11](#)

Deploying Configurations in Workflow Mode

When you deploy configurations in Workflow mode, you transfer the configurations directly to the devices in the network or to file in a specified output directory, depending on which option you chose when creating the job. See [Understanding Deployment Methods, page 18-11](#) for more information.

You deploy a job from the Deployment Status window, as described in the following procedure. The status of the deployment is displayed in the Status column of the Deployment Status window. See [Deployment Manager Window \(Workflow Mode\), page O-10](#). After a job is deployed, its devices become available for inclusion in other jobs.

You can view more detailed status information about the deployment in the Summary and Details tabs. See [Summary Tab \(Deployment Manager Window\), page O-34](#) and [Details Tab \(Deployment Manager Window\), page O-35](#) for more information.

**Caution**

You must configure at least one policy on a device before deploying to that device. If you deploy to a device without assigning at least one policy, the device's current configuration is overwritten with a blank configuration.

Notes

- Deployment might take from a few minutes to an hour or more, depending on the number of devices in the deployment job.
- Firewall devices only—After manually adding a firewall device or adding a device from DCR, we highly recommend that you discover (import) the factory-default policies for that device. Bringing these policies into Security Manager prevents you from unintentionally removing them the first time you deploy to that device. For more information about factory-default policies for firewall devices, see [Chapter 15, “Understanding Factory-Default Configurations.”](#) For more information about importing policies, see [Chapter 18, “Managing Deployment.”](#)

- The status of deployments to Catalyst 6500/7600 devices shows deployment to the device as well as its interface contexts when policy changes contain interface commands that affect the interface contexts (child devices). This can occur when you deploy a policy change that affects a VLAN in which the switch participates or when you update inventory, for example, by adding or deleting interface contexts.

Before You Begin

- Make sure that devices have been bootstrapped. For more information, see [Preparing the Devices for Security Manager to Manage, page 5-2](#).
- If you are deploying to a transport server, such as AUS, CNS, or TMS, make sure the server, Security Manager settings, and device have been set up properly.
- Create a job. For more information, see [Creating Deployment Jobs, page 18-51](#).
- If using Workflow mode with activity approval, submit the job. For more information, see [Submitting Deployment Jobs, page 18-55](#).
- Approve the job. For more information, see [Approving and Rejecting Deployment Jobs, page 18-56](#).

Procedure

-
- Step 1** Click the **Deployment Manager** button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Select the job to deploy.
- Step 3** Click **Deploy**.
The Deploy Job dialog box appears.
- Step 4** In the Deployment Options field, select when you want to deploy the job. Valid options are Schedule and Deploy Now.
If you choose Deploy Now, proceed to step 6. If you choose Schedule, the Enter Deployment Time field appears.
- Step 5** In the Deployment Time field, enter the date and time that you want the job to be deployed. For more details, see [Deploy Job Dialog Box, page O-27](#).
- Step 6** In the Deployment comments field, enter comments regarding the job.

Step 7 Click **OK**.

The Job Deployment Manager page appears. The job status changes to Deploying. When the deployment is complete, the job status changes to Deployed.

Related Topics

- [Including Devices in Deployment Jobs, page 18-10](#)
- [Understanding Deployment Methods, page 18-11](#)

Previewing Configurations

You can preview configurations from several different locations in Security Manager (see [Table 18-12](#)).

This procedure shows you how to display proposed configurations and compare them to last deployed configurations or current running configurations for specific devices, whether you are in Workflow mode or non-Workflow Mode.

Table 18-12 *Previewing Configurations*

| Workflow Modes | Action | Configuration Type |
|-------------------|--|------------------------------|
| Both | From Device view, right-click a device in the Device selector and select Preview Config. | Non-committed configuration |
| Both | From Maps view, right-click a device on the map and select Preview Config. | Non-committed configuration |
| Both | <ol style="list-style-type: none"> 1. Click Deployment Manager button in the Main toolbar. 2. Select a job. 3. Click Details tab. 4. Click the icon in the Config column for the desired device. | Last committed configuration |
| Non-Workflow mode | <ol style="list-style-type: none"> 1. Click File > Deploy. 2. Right click on a device in the device selector and select Preview config. | Committed configuration |

Table 18-12 *Previewing Configurations (continued)*

| Workflow Modes | Action | Configuration Type |
|-------------------|--|------------------------------|
| Non-Workflow mode | <ol style="list-style-type: none"> 1. Click File > Deploy. 2. Define job. 3. Click Deploy. 4. Click the icon in the Config column for the desired device. | Last committed configuration |
| Workflow mode | Right-click a device in the Device selector and select Preview config. | Committed configuration |
| Workflow mode | Select a device and click Preview Config. | Committed configuration |

The Configuration Preview dialog box appears. Click one of the following radio buttons to display configurations for comparison:

- None—Displays only the changed configuration on the device.
- Last Deployed—Displays the last configuration that was imported from the device and compares it with the proposed full configuration.
- Current Running—Displays the current configuration running on the device and compare it with the proposed full configuration.

For more information about the Preview Config dialog box, see [Preview Config Dialog Box, page O-21](#).

Changing Deployment Methods

The system default deployment method is to deploy to the device. You can set the default deployment method for all devices under **Tools > Security Manager Administration > Deployment**. For more details, see [Chapter 20, “Using Tools.”](#) In addition, you can change the deployment method for specific devices. If you are using non-Workflow mode, see [Deploying Configurations in Non-Workflow Mode, page 18-38](#). If you are using Workflow mode, see [Creating Deployment Jobs, page 18-51](#).

Refreshing Deployment Status Information

You can update the deployment status information at any time.

Procedure

- Step 1** Click the **Deployment Manager** button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Click **Refresh**.
Information in the window is updated.
-

Related Topics

- [Deployment Manager Window \(Non-Workflow Mode\)](#), page O-2
- [Deployment Manager Window \(Workflow Mode\)](#), page O-10
- [Job States in Non-Workflow Mode](#), page 18-4
- [Job States in Workflow Mode](#), page 18-8

Redeploying Configurations to Devices

You can redeploy any job. When redeploying a failed job, the devices that failed are automatically selected. However, you can also add devices to which deployment succeeded.



Caution

You must configure at least one policy on a device before deploying to that device. If you deploy to a device without assigning at least one policy, the device's current configuration is overwritten with a blank configuration.

Before You Begin

- Make sure that devices have been bootstrapped. For more information, see [Preparing the Devices for Security Manager to Manage](#), page 5-2.

- If you are deploying to a transport server, such as AUS, CNS, or TMS, make sure the server, Security Manager settings, and device have been set up properly.

Procedure

Step 1 Click the Deployment Manager button in the Main toolbar.

The Deployment Manager window appears.

Step 2 Select the job that contains the devices to which you want to redeploy configurations, then do one of the following:

- In non-Workflow mode, click **Redeploy**.
- In Workflow mode, click **Deploy**.

The Redeploy a Job dialog box appears.

Step 3 Select the rows corresponding to the devices to which you want to redeploy configurations.

Step 4 To change the deployment method, in the Method column, select one of the following deployment methods from the list:

- **Device**—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see [Deploying to a Device, page 18-11](#).
- **File**—Deploys the configuration file to a file on a selected server. If you select File, enter the directory to which you want to deploy the configuration file or click **Browse** to select from a list of available servers in the Destination column. For more information, see [Deploying to a File, page 18-13](#).



Note Before redeploying configurations to devices, you can preview proposed configurations and compare them against last deployed configurations or current running configurations. For more information, see [Previewing Configurations, page 18-43](#).

For a description of all elements displayed in the dialog box, see [Redeploy a Job Dialog Box, page O-32](#).

Step 5 Click **OK**.

Related Topics

- [Understanding Deployment Methods, page 18-11](#)
- [Preview Config Dialog Box, page O-8](#)
- [Job States in Non-Workflow Mode, page 18-4](#)
- [Job States in Workflow Mode, page 18-8](#)

Aborting Deployment Jobs

You can stop a job if you do not want to deploy the defined configuration file or you want to postpone deployment.

You can abort deployment jobs only while they are in the Deploying, Scheduled, or Rolling Back state. Aborting a job stops deployment of configuration files to pending devices, but has no effect on devices to which deployments are in progress (commands are being written to a device) or to which deployment has already completed successfully.

After you abort a job, the deployment status of pending devices changes to Aborted.

To resume deployment, redeploy the job. See [Redeploying Configurations to Devices, page 18-45](#) for more information.

Procedure

-
- Step 1** Click the Deployment Manager button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Select a deployment job, then click **Abort**.
A dialog box requests confirmation of the abort operation.
- Step 3** Click **Yes**.
-

Related Topics

- [Viewing Deployment Status Information, page 18-37](#)
- [Job States in Non-Workflow Mode, page 18-4](#)

- [Job States in Workflow Mode, page 18-8](#)

Rolling Back Configurations to Devices

If you deploy configurations to devices and then determine that there is something wrong with the new configurations, you can revert to and deploy the previous configurations for those devices.

You can also use the Config Archive tool to rollback to any configuration archived from a device. For more information, see [Using the Configuration Archive Tool, page 20-11](#).

Notes

- You cannot rollback to a previous configuration if the previous deployment was to a file or if there are no previous configurations.
- There is limited support for the rollback function on Catalyst 6500/7600 devices. VLAN configuration changes made through the CVDM home page are not captured in the running configuration of the Catalyst 6500/7600. Therefore, they are not included in the configurations saved to Security Manager database after each deployment. If you want to use the rollback function in this case, you need to reconfigure the VLANs on the CVDM home page after rolling back the configuration.
- Special considerations apply to the rollback of IPS devices and IOS IPS devices; see [Understanding Rollback for IPS and IOS IPS, page 20-19](#).

Before You Begin

- Make sure that devices have been bootstrapped. For more information, see [Preparing the Devices for Security Manager to Manage, page 5-2](#).
- If you are deploying to a transport server, such as AUS, CNS, or TMS, make sure the server, Security Manager settings, and device have been set up properly.
- For Catalyst 6500/7600 devices, you must enable a TFTP server on the Security Manager server, because for these two device types, the rollback is archived by transferring the configuration to the device (using TFTP) and then reloading it. In addition, you must set the TFTP root directory the same as the one set in Tools > Security Manager Administration > Config Archive.

Procedure

Step 1 Click the Deployment Manager button in the Main toolbar.

Step 2 Select a deployment job, then click **Rollback**.

A warning message appears.



Note The rollback operation causes the devices in the job to reload. If you *do not* want to reload devices, instead you can redeploy the job or create and deploy a new job with the desired configuration changes. Use the rollback operation only in extreme circumstances.

Step 3 To cancel the operation, click **Cancel**. To continue, click **OK**.

The Deployment Manager window appears.

Step 4 Select the devices for which you want to roll back configurations. By default, all the devices with the status “Succeeded” are selected.

The Rollback a Job dialog box appears. See [Deployment Rollback Dialog Box, page O-29](#) for a description of the elements in this dialog box.

Step 5 Click **Yes**.

Related Topics

- [Viewing Deployment Status Information, page 18-37](#)
- [Job States in Non-Workflow Mode, page 18-4](#)
- [Job States in Workflow Mode, page 18-8](#)

Viewing Deployment Summary Information

You can display summary information about deployment jobs, such as the job status, number of devices deployed successfully, and number of devices deployed with errors.

Procedure

- Step 1** Click the Deployment Manager button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Select a job.
Information about the selected job appears on the Summary tab. See [Summary Tab \(Deployment Manager Window\)](#), page O-34 for a description of the elements in this tab.
-

Related Topics

- [Viewing Deployment Device Details](#), page 18-50
- [Viewing Deployment Status Information](#), page 18-37

Viewing Deployment Device Details

While deployment is in progress, you can display deployment status details about specific devices.

Procedure

- Step 1** Click the Deployment Manager button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Select a job, then click the Details tab.
Information about the selected deployment job appears on the Details tab. See [Details Tab \(Deployment Manager Window\)](#), page O-35 for a description of the elements on the tab.
-

Related Topics

- [Viewing Deployment Summary Information](#), page 18-49
- [Viewing Deployment Status Information](#), page 18-37

Performing Additional Workflow-Mode Tasks

In Workflow mode, there are additional tasks that are performed to deploy configurations. The following topics provide information about these tasks:

- [Creating Deployment Jobs, page 18-51](#)
- [Opening and Closing Deployment Jobs, page 18-54](#)
- [Submitting Deployment Jobs, page 18-55](#)
- [Approving and Rejecting Deployment Jobs, page 18-56](#)
- [Discarding Deployment Jobs, page 18-57](#)
- [Viewing Deployment Job History, page 18-57](#)

Creating Deployment Jobs

Before you deploy policy configurations to your devices, you must create a deployment job. When you create a job, you specify parameters, such as the devices to which you want to deploy the configurations, whether you want to deploy directly to the devices or to an output file, and when you want the job to take place.

Notes

- If you choose to deploy the job immediately, deployment might take from a few minutes to an hour or more, depending on the number of devices in the deployment job.
- Firewall devices only—If you manually added a firewall device or added a device from DCR, we highly recommend that you discover (import) the factory-default policies for that device before deploying to that device. Bringing these policies into Security Manager prevents you from unintentionally removing them the first time you deploy to that device. For more information about factory-default policies for firewall devices, see [Chapter 15, “Understanding Factory-Default Configurations.”](#) For more information about importing policies, see [Chapter 18, “Managing Deployment.”](#)
- The status of deployments to Catalyst 6500 switches shows deployment to the device as well as its interface contexts when policy changes contain interface commands that affect the interface contexts (child devices). This can occur

when you deploy a policy change that affects a VLAN in which the switch participates or when you update inventory, for example, by adding or deleting interface contexts.

Before You Begin

- Make sure that devices have been bootstrapped. For more information, see [Preparing the Devices for Security Manager to Manage, page 5-2](#).
- If you are deploying to a transport server, such as AUS, CNS, or TMS, make sure the server, Security Manager settings, and device have been set up properly.

Procedure

-
- Step 1** Click the Deployment Manager button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Click **Create**.
The Create a Job dialog box appears.
- Step 3** In the Name field, a default name appears. Keep this name or enter a different, unique name for the deployment job. Because the job name enables you to distinguish one job from another, you should assign a logical name that reflect the contents of the job.
- Step 4** In the Description field, enter some information that reflects the contents of the job.
- Step 5** Select the devices to which you want to deploy configurations.
- Step 6** To change the method used to deploy configurations to specific devices, click **Edit Deploy Method**.



Note The system default deployment method is Device unless it has been changed under Tools > Security Manager Administration. To change the system-wide default deployment method, see [Chapter 20, “Using Tools.”](#)

The Edit Deployment Method dialog box appears.

- a. Select the row corresponding to the device for which you want to change the deployment method.

- b. In the Method column, select one of the following deployment methods from the list:
- Device—(Default) Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see [Deploying to a Device, page 18-11](#).
 - File—Deploys the configuration file to a file on a selected server. If you select File, enter the directory to which you want to deploy the configuration file or click **Browse** to select from a list of available servers in the Destination column. For more information, see [Deploying to a File, page 18-13](#).



Note Before deploying to devices, you can preview proposed configurations and compare them against last deployed configurations or current running configurations. For more information, see [Previewing Configurations, page 18-43](#).

For a description of all elements displayed in the dialog box, see [Edit Deploy Method Dialog Box, page O-17](#).

- Step 7** To add devices that do not have proposed policy changes to the deployment job, click **Add other devices**. For example, you might want to do this if a device was manually modified, and you want to return the device to its previous configuration (the one stored in the Security Manager database).

The Add Devices dialog box appears, listing *all* devices whether or not they contain proposed policy changes.

- a. Select the check box next to the devices to include in the job; then click >> to move the devices to the Selected Devices field.
- b. Click **OK**.

For a description of all elements displayed in this dialog box, see [Add Other Devices Dialog Box, page O-23](#).

- Step 8** To select the state of the job when you are done, click one of the following radio buttons:

- Leave the job in the edit state—Saves the job so that you can make additional changes later.
- Approve the job—Approves the job so that it can be deployed later. If you click this option, you can add approval comments.

- Deploy the job—Deploys the job. If you click this option, you can select whether to deploy the job now or schedule it for a later time, and you can add deployment comments.

Step 9 Click **OK**.

The status of the deployment job depends on the state you selected in the previous step.

Related Topics

- [Including Devices in Deployment Jobs, page 18-10](#)
- [Understanding Deployment Methods, page 18-11](#)

Opening and Closing Deployment Jobs

If you want to make changes to a deployment job, you must open the job. The job status changes to Edit Open.

Normally, you do not need to close a job, because you will typically submit, approve, deploy, or schedule the job for deployment. However, if the Security Manager server is suddenly unavailable or your login session times out, a job might be left in the Edit Open state. If this happens, you can close it manually.

Procedure

Step 1 Click the Deployment Manager button in the Main toolbar.

The Deployment Manager window appears.

Step 2 Select a job and do one of the following:

- Click **Open** to open the job.
- Click **Close** to close the job.

The Deployment Manager window appears.

Related Topics

- [Deployment Manager Window \(Workflow Mode\), page O-10](#)

- [Job States in Workflow Mode, page 18-8](#)

Submitting Deployment Jobs

In some organizations, before jobs can be deployed, they must be approved by a separate user with the appropriate permissions. In this case, Workflow mode is enabled *with* a deployment job approver, and you must submit the job to this user for review. The user reviews the job and either approves or rejects it.

If you are using Workflow mode *without* a deployment job approver, you can review and approve the job yourself. Submitting the job submits and approves the job in one step.



Note

You enable and disable deployment job approval under Tools > Security Manager Administration > Workflow. For more information, see [Chapter 2, “Performing Administrative Tasks.”](#)

Procedure

Step 1 Click the Deployment Manager button in the Main toolbar.

The Deployment Status window appears.

Step 2 Select the job to submit.

Step 3 Click **Submit**.

In Workflow mode *with* a deployment job approver, the job status changes to Submitted. In Workflow mode *without* a deployment job approver, the job status changes to Approved.

Related Topics

- [Deployment Manager Window \(Workflow Mode\), page O-10](#)
- [Job States in Workflow Mode, page 18-8](#)

Approving and Rejecting Deployment Jobs

In some organizations, before jobs can be deployed, they must be approved by a separate user with the appropriate permissions. In Workflow mode *with* a deployment job approver, one user submits a job, and another one previews the job and either approves or rejects it.

In Workflow mode without a deployment job approver, you can create and approve the job at the same time. For more information, see [Creating Deployment Jobs, page 18-51](#).

When you reject a job, the devices in the job immediately become available for inclusion in other jobs. A rejected job cannot be deployed, but it can be opened for viewing and editing.

**Note**

You enable and disable deployment job approval under Tools > Security Manager Administration > Workflow. For more information, see [Chapter 2, “Performing Administrative Tasks.”](#)

Procedure

Step 1 Click the Deployment Manager button in the Main toolbar.

The Deployment Manager window appears.

Step 2 Select a submitted job and do one of the following:

- Click **Approve**.
- Click **Reject**.

The job status changes to Approved or Rejected, as appropriate.

Related Topics

- [Deployment Manager Window \(Workflow Mode\), page O-10](#)
- [Job States in Workflow Mode, page 18-8](#)

Discarding Deployment Jobs

You can discard a job when it is in any state except Deployed, Deployment Failed, or Aborted. The job state is shown as discarded until the job is purged from the system, either automatically as set on the Workflow Management page or manually.

Procedure

- Step 1** Click the Deployment Manager button in the Main toolbar.
The Deployment Manager window appears.
 - Step 2** Select the job to discard.
 - Step 3** Click **Discard**.
 - Step 4** In the Comment field, enter a comment explaining why you are discarding the job.
 - Step 5** Click **OK**.
-

Related Topics

- [Deployment Manager Window \(Workflow Mode\), page O-10](#)
- [Job States in Workflow Mode, page 18-8](#)

Viewing Deployment Job History

The Deployment Job History tab displays transactions that occurred to the selected job since it was created. Each row in the table shows the action that occurred, the user who performed the action, the date and time it occurred, and comments, if any, that the user entered.

Procedure

- Step 1** Click the Deployment Manager button in the Main toolbar.
The Deployment Manager window appears.
- Step 2** Select the desired job.
- Step 3** Click the History tab.

Information about the transactions that occurred during the deployment are displayed. See [History Tab \(Deployment Manager Window\)](#), page O-36 for information about the elements in this tab.

**Note**

The timestamps shown on the History tab use the timezone of the server, not the timezone of the client.

Related Topics

- [Deployment Manager Window \(Workflow Mode\)](#), page O-10
- [Viewing Deployment Summary Information](#), page 18-49
- [Viewing Deployment Device Details](#), page 18-50

