# 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 Workflow and Activities Overview.

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



# 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. You can also create deployment schedules to automatically spawn deployment jobs at regular intervals.

The following topics will help you better understand and use deployment jobs:



## Overview of the Deployment Process

Broadly speaking, deployment is a three-step process, as described in the following table.

*Table 1: Overview of the Deployment Process*

| Steps | 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 to be 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:<br>• Obtain the running configuration from the device.<br><br>The running configuration is 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**).<br>• Obtain the last full configuration from the Security Manager Configuration Archive. The Configuration Archive is used when:<br>• Deploying to file, unless you select **When Deploying to File Get Reference Config from: Device** as the deployment preference.<br>• The deployment method is TMS or CNS.<br>• The device is not managed by Security Manager.<br>• 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.<br>• You preview configurations.<br>• Use the factory default configuration.<br><br>The factory default configuration is used with PIX or ASA devices if you use the AUS deployment method. It is used for deployment and for configuration preview. |
| **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. |

| Steps | Deployment Steps |
|---|---|
| **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 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:<br>• SSL (HTTPS), SSH, or Telnet—Security Manager contacts the device directly and sends the delta configuration to it.<br>• 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.<br>• Configuration Engine for IOS devices—Security Manager sends the delta configuration to Configuration Engine, where the device retrieves it.<br>• 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. |

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 Band 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. This is the recommended approach.

For more information on how out-of-band changes affect deployment, see Understanding How Out-of-Band Changes are Handled , on page 12.

After configurations are deployed, you should make changes only through Security Manager for configurations that Security Manager controls. This varies based on operating system. For IPS devices, Security Manager controls the entire configuration. For IOS, ASA, PIX, and FWSM devices, you have more control over which aspects of the device configuration Security Manager controls. 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 these devices, thereby preventing Security Manager from displaying or changing policies for these features. To see the available features and control whether they are available for management in Security Manager, select **Tools > Security Manager Administration**, then select **Policy Management**. Security Manager does manage VPN-related policies.

### Related Topics

- Deployment in Non-Workflow Mode , on page 4
- Deployment Task Flow in Workflow Mode , on page 5
- Deployment Page
- Policy Management Page

# Deployment in Non-Workflow Mode

These topics help you understand deployment in non-Workflow mode:

- Deployment in Non-Workflow Mode , on page 4
- Job States in Non-Workflow Mode , on page 5

## Deployment Task Flow in Non-Workflow Mode

The deployment task flow in non-Workflow mode consists of three simple steps:

1. **Create the 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, or select **File > Submit and Deploy**.

**Note** These options are not available when Ticket Management is enabled.

   - Select **File > Deploy**.
   - Select **Manage > Deployments** and click **Deploy**.

1. **Define the 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 in which policies are deployed is correct. However, you can include devices that are specified in deployment schedules.

2. **Deploy the job:** Deploying the job sends the generated CLI to devices, either directly or through an intermediary transport server (such as AUS, CNS, or TMS) or to output files. You select the destination (device or file) when defining a job. The transport server is specified in the device properties. For more details about defining deployment methods and transport servers, see Understanding Deployment Methods , on page 9.

## Job States in Non-Workflow Mode

In non-Workflow mode, the Status column on the Deployment Manager window lists the state of each job. The following table lists and describes all possible job states in non-Workflow mode. For more details, see Deployment Manager Window , on page 15.

***Table 2: 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 configuration 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 a directory on the Security Manager server. You can monitor the job progress in the Deployment Manager window if the Deployment Status window is not already open. |
| Aborted | The job was manually halted. Devices in the job can now be included in another job. |
| Failed | The 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

The following is a typical task flow in Workflow mode (see Figure 1: Deployment Task Flow in the Workflow Mode, on page 6):

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

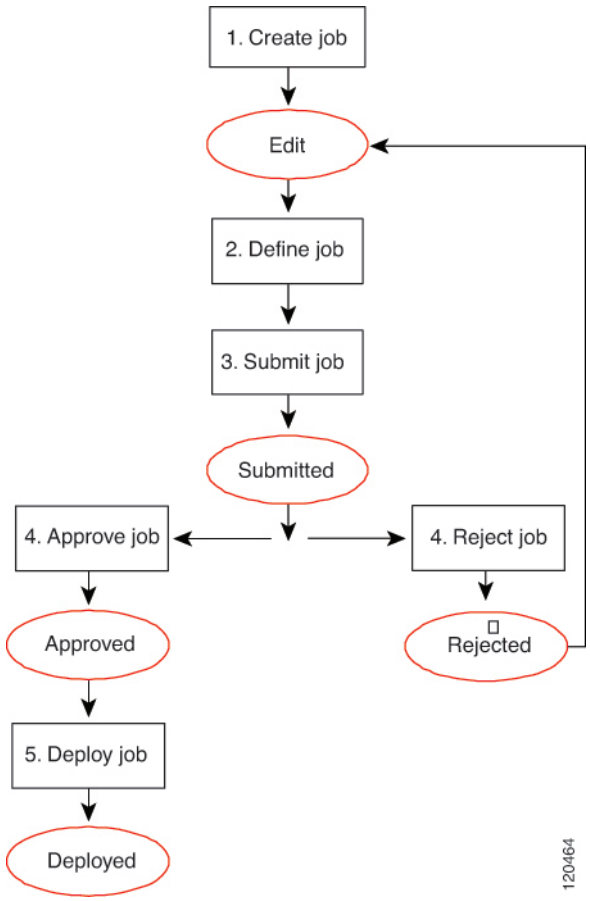
4. **Approve or reject the job:** If you are working in Workflow mode with a deployment job approver, the approver reviews it, and can then either approve or reject the job. If the job is approved, the submitter can then deploy the job. If the job is rejected, the submitter can discard the job and start over or modify the job and resubmit it.

If you are working in workflow mode without an approver, you can approve the job yourself.

- **Deploy the job:** Deploying the job sends the generated CLI to either devices, intermediary transport servers (such as AUS, CNS, or TMS), or files. You select the destination (device or file) when defining the job. The transport server is specified in the device properties. For more details about defining deployment methods and transport servers, see Understanding Deployment Methods , on page 9.

For descriptions of job states (shown in red in Figure 1: Deployment Task Flow in the Workflow Mode, on page 6), see Job States in Workflow Mode , on page 7.

***Figure 1: Deployment Task Flow in the Workflow Mode***



# Job States in Workflow Mode

In Workflow mode, the Status column in the Deployment Manager window lists the state of each job. The following table lists and describes all possible job states. For more details about the Deployment Manager window, see Deployment Manager Window , on page 15.

***Table 3: Job States in Workflow Mode***

| State | Description |
|---|---|
| Edit | The job was created, but it is not currently being edited. The job can be opened, approved (in auto-approval mode), or discarded while it is in the Edit state. |
| Edit-In Use | The job is open for editing. The job can be closed, approved, discarded, or submitted while it is in the Edit Open state. |
| Submitted | The 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. This state occurs only when Workflow mode is enabled with deployment job approval required. |
| Approved | The job was approved and is ready to be deployed. The job can be deployed while it is in the Approved state. |
| Rejected | The job was rejected. You can open the job for editing or discard the job while it is in the Rejected state. This state occurs only when Workflow mode is enabled with deployment job approval required. |
| Discarded | The job was discarded. No 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 be included in another job. |
| Deployed | Configurations for all the devices in the job were successfully deployed to the devices or to configuration 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 a directory on the Security Manager server. You can monitor the job progress in the Deployment Manager window. |
| Aborted | The job was manually halted. Devices in the job can now be included in another job. |
| Failed | The 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] | The 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. |

## 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 Workflow Page.

## 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 or Schedules

When you create a deployment job or schedule, you select the devices to include in it. The inclusion of a device influences how the device can be used in other jobs or schedules. When you select a device for a specific job, it cannot be selected for any other job until the original job is deployed, rejected (in 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.

However, a device can be part of a deployment schedule and still be selected for specific deployment jobs. While a deployment job is running, the device is locked. The device cannot be included in other jobs while the deployment job is running.

When you create a deployment job, Security Manager displays the devices on which policy changes were made but were not yet deployed. You can deploy to these devices, and you can select additional devices for the job. Although you can add as many devices to a deployment job as you desire (there is no limitation), as a practical matter, you should limit the number of devices per job. The deployment job might fail if you select a large number of devices or several devices that have large configuration files. If you encounter deployment failures, resubmit the job with fewer devices selected.

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 property.

# Understanding Deployment Methods

Security Manager lets you deploy configurations to devices using three main methods: deploying directly to the device, deploying to a configuration file (which you must then manually apply to the device), and deploying to an intermediate server (which is treated like deploying directly to the device). The system default deployment method is to deploy directly to the device.

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**; see Deployment Page). 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. If you are using non-Workflow mode, see Deploying Configurations in Non-Workflow Mode , on page 28. If you are using Workflow mode, see Creating and Editing Deployment Jobs , on page 35.

The method you choose to use depends on the processes and procedures of your organization and the transport protocols supported by a particular type of device. 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 (HTTPS) for IOS, PIX, ASA, IPS, and standalone FWSM devices, and SSH for FWSM through the Catalyst chassis. If you are using a Token Management Server (TMS) for some devices, you can also use that method with Security Manager.

The following topics describe the deployment methods in more detail:



## Deploying Directly to a Device

If you choose to deploy directly to a device, Security Manager uses the transport protocol defined in the device properties for the device (right click the device, select **Device Properties**, and click **General**). The protocol is typically the default protocol defined in the Device Communication page in the Security Manager Administration settings (see Device Communication Page). Table 4: Default Deployment Transport Protocols , on page 10 lists some of the default transport protocol settings.

When you select Device as the deployment method, deployment is affected if you configure a transport server for the device, such as an AUS or Configuration Engine. When using an intermediate transport server, configuration deployment goes through the server. For more information on using an intermediate server, see Deploying to a Device through an Intermediate Server , on page 10.

Deployment can also be affected if you made out-of-band changes to the device since the last deployment. For more information, see Understanding How Out-of-Band Changes are Handled , on page 12.

During deployment, Security Manager sends only the changes made since the last deployment to the device.

**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 4: Default Deployment Transport Protocols***

| Device Type | Transport Protocol | Description |
|---|---|---|
| ASA, IOS 12.3 and later routers, FWSM, PIX Firewall, IPS sensors | SSL (HTTPS) (Default) | Security Manager deploys the configuration to the device using the Secure Socket Layer (SSL) protocol, otherwise known as HTTPS. With this protocol, Security Manager encrypts the configuration file and sends it to the device. |
| Catalyst 6500/7600 and other Catalyst switches | SSH | 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. |
| IOS 12.2 and 12.1 routers | Telnet | Security Manager deploys the configuration to the device using the Telnet protocol. |

### Related Topics

- Managing Device Communication Settings and Certificates
- Handling Device OS Version Mismatches , on page 13

## Deploying to a Device through an Intermediate Server

Deploying configurations through an intermediate server, such as an Auto Update Server (AUS), Cisco Networking Services (CNS) Configuration Engine, or Token Management Server (TMS), is a version of deploying directly to device. When selecting the deployment method, select Device. Security Manager sends the configuration updates to the intermediate server, where the device retrieves it (for AUS and CNS), or where you can download it to an eToken (for TMS).

You must use an intermediate server if you are using dynamic IP addresses for your device interfaces (that is, the IP addresses are provided by a DHCP server). You can also use them with static IP addresses. However, you cannot use Configuration Engine to manage IOS devices with dynamic IP addresses if you configure features that use interactive CLI commands. The following features are affected:

- Certificate Enrollment:
  - **crypto pki trustpoint**
  - **crypto isakmp client configuration group**
  - **crypto key generate rsa**

- IPS signature configuration (**ip ips signature-category**)
- IP Authproxy Banner (**ip auth-proxy-banner**)
- Catalyst device interface switchport (**interface switchport**)

Security Manager uses an intermediate server if you have configured the device to use one. The following topics describe the required configuration steps when using an intermediate server:

- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42
- Deploying Configurations to a Token Management Server , on page 43

Deployment can be affected if you made out-of-band changes to the device since the last deployment. For more information, see Understanding How Out-of-Band Changes are Handled , on page 12.

During deployment, Security Manager sends configuration changes based on the type of server:

- 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.
- 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.

### Related Topics

- Managing Device Communication Settings and Certificates
- Device Communication Page

## Deploying to a File

If you choose to deploy configurations to configuration files, Security Manager creates two files: *device_name* _delta.cfg for the delta configuration, and *device_name* _full.cfg for the full configuration. If the files are created by a job that was generated from a deployment schedule, the name includes a time stamp. Configuration files are in TFTP format so that you can upload them to your devices using TFTP.

**Tip** You cannot deploy configurations to file for IPS devices.

If you deploy to file, you are responsible for transferring 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. 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.

**Caution** Although Security Manager in one sense assumes that you applied the delta configuration, in another sense, it assumes that it cannot know if the delta was deployed. Thus, Security Manager maintains an internal view of the configuration based on the last deployment made directly to the device. So, when you apply the delta, those delta changes will be considered out-of-band changes. On next deployment to the device, your out-of-band change setting might cancel the deployment. If you mix deployments to file with deployments to device, you should rediscover policies after applying file deployments to the device. For more information, see Understanding How Out-of-Band Changes are Handled , on page 12.

To set a default directory for file deployments, select **Tools > Security Manager Administration**, then select **Deployment** (see Deployment Page). 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.

Deploying configurations to a file is useful when the devices are not yet in place in your network (known as green field deployment), if you have your own mechanisms in place to transfer configurations to your devices, or if you want to delay deployment. When deploying to a file, the deployment job might fail if you select a large number of devices or several devices that have large configuration files. If you encounter deployment failures, resubmit the job with fewer devices selected.

**Tip** Do not use commands that require interaction with the device during deployment 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 , on page 44.

## Understanding How Out-of-Band Changes are Handled

Security Manager considers an out-of-band change to be any change made to a device manually or outside of Security Manager control, for example, by logging into the device directly and entering configuration commands through the CLI. Paradoxically, this includes the application of delta changes that Security Manager creates when you deploy configurations to file rather than to the device.

If you are deploying to the device (rather than to file), and the deploy to device method is configured to compare the new configuration to the current configuration on the device, you can specify how to handle out-of-band changes when they are detected using the **Out of Band Change Behavior** setting. The setting does not apply when deploying to file.

This setting is ignored if you are comparing the new device configuration with the latest version stored in the Security Manager Configuration Archive. The default way to handle out-of-band changes, is set in Tools > Security Manager Administration > Deployment; for more information see Deployment Page. Look for the **Deploy to Device Reference Configuration** and **When Out of Band Changes Detected** settings.

Your options for handling out-of-band changes are:

- **Overwrite changes and show warning**—When configurations are deployed, 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, Security Manager continues with the deployment and displays a warning notifying you of this action. Out-of-band changes are removed from the device.
- **Cancel deployment**—When configurations are deployed, 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, Security Manager cancels the deployment and displays a warning notifying you of

this action. You must either manually remove the out-of-band changes, or configure the same settings in Security Manager, before you can deploy configuration changes to the device.

- **Do not check for changes**—Security Manager does not check for changes and deploys the changes to the device. No warnings are issued, and any out-of-band changes are removed from the device configuration.

Before you deploy configurations, you might want to detect whether there are out of band changes on a device and analyze whether you want to recreate those changes in Security Manager policies, or allow Security Manager to overwrite the changes. For more information, see Detecting and Analyzing Out of Band Changes , on page 46.

### Related Topics

- Deploying Directly to a Device , on page 9
- Deploying to a Device through an Intermediate Server , on page 10
- Deploying to a File , on page 11

# Handling Device OS Version Mismatches

Before deploying a changed configuration file directly to a device, Security Manager normally 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 (you can configure it so that the archived configuration is used instead of the configuration from the device). Security Manager takes action depending on whether the OS versions match or differ from each other.

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, ASA 8.1(2) instead of the 8.1(1), indicated in Security Manager.
- The device has a down-level minor version, for example, ASA 8.1(1) instead of 8.1(2).

Security Manager does not deploy the configuration when the device is running a new major version of the OS (for example, ASA 8.0 instead of the 7.2 indicated in Security Manager) or if the device is running a down-level major version (7.2 instead of 8.0).

The following table lists the possible actions Security Manager takes depending on the whether the OS versions match or differ from each other. The table uses the ASA device as an example; however, the actions apply to all supported device types.

***Table 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 | ASA 8.2(1) | ASA 8.2(1) | ASA 8.2(1) | Deployment proceeds with no warnings. |

| Scenario | OS Version in Security Manager Database | OS Version On Device | OS Version Used In Deployment | Action |
|---|---|---|---|---|
| Device has newer minor OS version. | ASA 8.1(1) | ASA 8.1(2) | ASA 8.1(2) | Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.<br>Security Manager generates the CLI based on the OS version running on the device. |
| Device has newer minor OS version, one that is not directly supported by Security Manager. | ASA 8.0(2) | ASA 8.0(4) | ASA 8.0(3) | Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.<br>Security Manager generates the CLI based on the OS version that it supports to which the running OS version is downward-compatible. |
| Device has a new major OS version. | ASA 7.2(4) | ASA 8.2(1) | None. Deployment fails. | 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.<br>Security Manager cannot proceed until you correct this mismatch. Remove the device from the inventory, add it again, and discover the device policies. |
| Device has an older minor OS version. | ASA 8.1(2) | ASA 8.1(1) | ASA 8.1(1) | Security Manager warns that it has detected a different OS version on the device than the one in the Security Manager database.<br>Security Manager generates the CLI based on the OS version running on the device. |
| Device has an older major OS version | ASA 8.2(1) | ASA 7.2(4) | None. Deployment fails. | 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.<br>Security Manager cannot proceed until you correct this mismatch. Remove the device from the inventory, add it again, and discover the device policies. |

# Overview of the Deployment Manager and Configuration Archive

The Deployment Manager and Configuration Archive are the main tools that you can use to manage deployment and device configurations. The following topics provide an overview of these tools:

# Understanding What You Can Do with the Deployment Manager

The Deployment Manager, where you create and manage deployment jobs and schedules, provides the following benefits:

- 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 the device or what is currently running on the device.

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 , on page 44.

- Aborting deployment jobs—You can stop a deployment job even if it is currently running. However, aborting a job that is in process does not roll back the configuration on devices that have already been reconfigured, or on devices that are in the process of being reconfigured. Only devices for which deployment has not started are prevented from being reconfigured. For more information, see Aborting Deployment Jobs , on page 56.
- 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 Using the Deployment Manager , on page 72.
- Viewing deployment job status—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 Status and History for Jobs and Schedules , on page 25.
- Scheduling deployment jobs—You can create deployment schedules to spawn deployment jobs at regular intervals. In Workflow mode, you can also schedule a deployment job to start at a future time when you deploy the job. Scheduling jobs lets you plan deployments for times when traffic on devices is low. For more information, see these topics:
  - Creating or Editing Deployment Schedules , on page 56
  - Deploying a Deployment Job in Workflow Mode , on page 40
- Logging deployment job history (Workflow mode only)—You can view the history of transactions for a job. The transactions show the changes in job status initiated by various users, such as job approval, and the comments related to those status changes. For more information, see Viewing Deployment Status and History for Jobs and Schedules , on page 25.

# Deployment Manager Window

Use the Deployment Manager window to manage deployment jobs and schedules. You can display a list of deployment jobs, view job details, deploy and redeploy configurations to devices, abort deployment jobs, roll

back to previous configurations on selected devices, and create schedules to automatically generate deployment jobs. You can also track changes made to deployment jobs and schedules.

**Note** The buttons available in the Deployment Manager depend on the Workflow mode you are using.

### Navigation Path

Click the **Deployment Manager** button on the Main toolbar or select **Manage** > **Deployments**.

### Related Topics

- Overview of the Deployment Process , on page 1
- Viewing Deployment Status and History for Jobs and Schedules , on page 25
- Deploying Configurations in Non-Workflow Mode , on page 28
- Deploying a Deployment Job in Workflow Mode , on page 40
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42
- Deploying Configurations to a Token Management Server , on page 43
- Managing Device Communication Settings and Certificates

### Field Reference

*Table 6: Deployment Manager Window (Workflow Mode)*

| Element | Description |
|---|---|
| **Deployment Jobs Tab**<br>This tab shows individual deployment jobs. Select a job in the upper pane to view its details in the tabs in the lower pane.<br>Filter Options<br>Beginning with 4.14, Cisco Security Manager provides filter options to search deployment jobs based on Name (deployment job name), Status, Changed By, and Device Name. After specifying the filter criteria, click Apply. The grid displays the search result. Select a job in the table to view its details in the tabs in the lower pane. | |
| Name | The name of the job. |
| Last Action | The date and time that the job or status was changed based on the time zone of the server, not the time zone of the client. |
| Status | The state of each job. The possible states differ based on workflow mode. For a description of the states, see the following topics:<br>• Job States in Non-Workflow Mode , on page 5<br>• Job States in Workflow Mode , on page 7 |

| Element | Description |
|---|---|
| Changed By | The name of the user who modified the job. |
| Description | The description of the job. Double-click the icon to see the description in a separate dialog box. |
| Job Type | The type of job with respect to scheduling. A **one time** job was not created from a regularly recurring job, whereas a **recurring** job was. |
| Create button<br>(Workflow mode only.) | In Workflow mode, click this button to create a new job. The Create a Job dialog box opens. See Creating and Editing Deployment Jobs , on page 35. |
| Open button<br>(Workflow mode only.) | In Workflow mode, click this button to open the selected job. The Edit a Job dialog box opens. See Creating and Editing Deployment Jobs , on page 35. |
| Close button<br>(Workflow mode only.) | In Workflow mode, click this button to close and save all changes made while the selected job was open. You can close a job when it is in the Edit Open or the Submit Open state. 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 by selecting it and clicking Close. |
| Submit button<br>(Workflow mode only.) | In Workflow mode, click this button to submit the selected job for approval. You can submit a job when it is in the Edit or the Edit Open state. The Submit Deployment Job dialog box opens. See Submitting Deployment Jobs , on page 38.<br>This button is active only if you are using Workflow mode with a deployment job approver. |
| Reject button<br>(Workflow mode only.) | In Workflow mode, click this button to reject the selected job if you are not satisfied with the configurations generated for the devices. You can reject jobs only in workflow mode with a deployment job approver. After a job is rejected, it can be opened for editing or discarded. See Approving and Rejecting Deployment Jobs , on page 39.<br>You are prompted to enter an optional comment to explain why you are rejecting the job. |
| Approve button<br>(Workflow mode only.) | In Workflow mode, click this button to approve the selected job. After a job is approved, it can be deployed. See Approving and Rejecting Deployment Jobs , on page 39.<br>You are prompted to enter an optional comment to explain why you are approving the job. |

| Element | Description |
|---|---|
| Discard button<br>(Workflow mode only.) | In Workflow mode, click this button to discard the selected job. You can discard a job when it is in any state except Deployed, Deployment Failed, or Aborted. Once discarded, the job cannot be edited, submitted, approved, or deployed. The job state is shown as discarded until the job is purged from the system either automatically as set on the Workflow settings page or manually (for more information, see Workflow Page.<br>You are prompted to enter an optional comment to explain why you are discarding the job. See Discarding Deployment Jobs , on page 41. |
| Deploy button<br>(All modes.) | Click this button to deploy generated CLI commands devices or files. The behavior of this button differs depending on Workflow mode:<br>• (Non-Workflow mode.) Click this button to create a deployment job. If you have unsubmitted changes, you are first prompted to submit them. The Deploy Saved Changes dialog box opens, where you can select which devices to include in the job. Note that this button does not act on the deployment job selected in the table, if any; instead, it creates a new deployment job. See Deploying Configurations in Non-Workflow Mode , on page 28.<br>• (Workflow mode.) Click this button to deploy the selected job. If the job is in the Approved state, the Deploy Job dialog box opens (see Deploying a Deployment Job in Workflow Mode , on page 40).<br>If the job is in the deployed, failed, or aborted state then the Redeploy Job dialog box opens. See Redeploying Configurations to Devices , on page 54. |
| Generate Report button<br>(All modes.) | Click this button to create a deployment status report for the selected job. You can generate the report in HTML and PDF formats. Jobs must be in deployed, failed, rolled back, or aborted state.<br>The deployment status report includes a summary of the job plus the full and delta configurations and the job transcript. You can use this report for your own purposes or to aid in troubleshooting a problem with Cisco TAC. For more information, see Generating Deployment or Discovery Status Reports. |
| Refresh button<br>(All modes.) | Click this button to reload job information from the Security Manager server. If the message *Auto Refresh is On* is displayed beneath the table, the job list is automatically refreshed periodically.<br>**Note** The auto refresh setting is configured in the administration settings for deployment: select **Tools > Security Manager Administration > Deployment**. |
| Redeploy button<br>(Non-Workflow mode only.) | In Non-Workflow mode, click this button to redeploy the selected job, which deploys the same generated CLI commands to the same devices or files selected in the original job. The Redeploy Job dialog box opens. See Redeploying Configurations to Devices , on page 54.<br>(In Workflow mode, click the Deploy button to redeploy configurations for the selected job.) |

| Element | Description |
|---|---|
| Abort button<br>(All modes.) | Click this button to abort the selected job if it is in the Deploying, Scheduled, or Rolling Back state. A warning asks you to confirm the action. See Aborting Deployment Jobs , on page 56. |
| Rollback button<br>(All modes.) | Click this button to deploy the previously deployed configuration to the devices in the selected job. The Deployment Rollback dialog box opens (see Rolling Back Configurations to Devices Using the Deployment Manager , on page 72). |
| Summary tab | Displays summary information about the status of the selected deployment job, such as the status of the job, the name of the deployment job, the number of devices included in the job, the number of devices deployed successfully, and the number of devices deployed with errors. |
| Details tab | Displays detailed information for the selected job. The table lists each device included in the job, whether deployment succeeded or failed, the tickets containing changes that are part of the job for the device, and a summary of the number of warnings, errors, or failures for the device. Select a device in the table to view the results for that device:<br>• Double-click the icon in the Config column to view the configuration (see Previewing Configurations , on page 44). If you deleted the device from the inventory, the configuration and transcript might not be available.<br>• If you were deploying to the device, double-click the icon in the Transcripts column to view a transcript of the commands sent to the device and the device's responses. See Viewing Deployment Transcripts , on page 64.<br>• If Ticket Management is enabled, the Last Ticket(s) column displays the ticket IDs of the tickets containing changes that are part of the deployment for the device. You can click on the Ticket IDs to view additional information about the ticket, such as Creator and Last Modified date. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page).<br>• When you select a device, the Messages box in the lower left contains a summary of the messages generated for the deployment. Select an item to view its description to the right. You might have to enlarge the window to make the Description box visible. If applicable, there might also be information on the actions you can take to resolve the problems. |
| History tab<br>(Workflow mode only.) | Displays a log of the changes that have been made to the selected job. The information includes the state changes, the user who made the change, the date and time of the change (based on the Security Manager server time), and any comments the user entered to document the change. |
| **Deployment Schedules Tab**<br>Use this tab to schedule regular deployment jobs. For detailed information about this tab, see Deployment Schedules Tab, Deployment Manager , on page 20. | |

## Deployment Workflow Commentary Dialog Box

When you perform an action in the Deployment Manager while working in Workflow mode, you are prompted to enter a comment to describe the action. The comments are preserved in the history for the job or schedule.

The title of the dialog box indicates the action you are taking. Enter an optional comment and click **OK** to perform the action.

### Navigation Path

In Workflow mode, select a job or schedule in the Deployment Manager and click the appropriate button to perform the desired action.

# Deployment Schedules Tab, Deployment Manager

Use the Deployment Schedules tab on the Deployment Manager window to create regularly recurring deployment jobs. Whenever the scheduled deployment time occurs, Security Manager creates a specific deployment job based on the scheduled job.

### Navigation Path

Click the **Deployment Manager** button on the Main toolbar or select **Manage** > **Deployments**, and then click the **Deployment Schedules** tab in the upper pane.

### Related Topics

- Overview of the Deployment Process , on page 1
- Creating or Editing Deployment Schedules , on page 56
- Suspending or Resuming Deployment Schedules , on page 60

### Field Reference

*Table 7: Deployment Schedules Tab, Deployment Manager Window*

| Element | Description |
|---|---|
| **Deployment Schedule Table**<br>This table shows deployment job schedules. Select a schedule in the table to view its details in the tabs in the lower pane.<br>Filter Options<br>Beginning with 4.14, Cisco Security Manager provides filter options to search deployment schedules based on Name (deployment schedule name), Status, and Device Name. After specifying the filter criteria, click Apply. The grid displays the search result. Select a schedule in the table to view its details in the tabs in the lower pane. | |
| Name | Name of the job schedule. Jobs created from this schedule use this name plus a time stamp. |

| Element | Description |
|---|---|
| Status | The status of the schedule:<br>• Edit—In Workflow mode, the schedule is being created. You can open it and change its settings. No jobs are created from schedules that are being edited.<br>• Active—Deployment jobs will be created according to this schedule.<br>• Suspended—The schedule was suspended and no jobs are being created by it. You can restart the schedule by selecting it and clicking **Resume**. |
| Recurrence | How often deployment jobs will be created from this schedule. |
| Next Run | The date and time a deployment job will next be created from this schedule. |
| Last Run | The date and time of the most recent deployment job created from this schedule. |
| Schedule End | The date and time the schedule is no longer active. If the schedule has no end date, Active Indefinitely is indicated. |
| Description | The description of the job schedule. Double-click the icon to see the description. |
| Create button | Click this button to create a deployment job schedule. The Schedule dialog box opens where you can create the schedule (see Schedule Dialog Box , on page 58. |
| Open button | Click this button to open the selected schedule. The Schedule dialog box opens where you can view or modify the schedule (see Schedule Dialog Box , on page 58).<br>In non-Workflow mode, modifying the schedule does not change its status. In Workflow mode, the status changes to Edit, and you must resubmit it for approval. |
| Close button<br>(Workflow mode only) | Click this button to close and save all changes made while the schedule was open. You can close a schedule when it is in the Edit Open or the Submit Open state. Typically, you will have to close schedules only if the Security Manager server becomes unavailable while you have a schedule open. |
| Submit button<br>(Workflow mode only) | Click this button to submit the selected schedule for approval if you are operating in Workflow mode with an approver. You can submit a schedule when it is in the Edit or the Edit Open state. You are prompted for an optional comment to explain the submission, and an e-mail is generated to the approver in Workflow mode. |
| Reject button<br>(Workflow mode only) | Click this button to reject the selected schedule. You are prompted for an optional comment to explain the rejection, and an e-mail is generated to the approver and submitter in Workflow mode. |
| Approve button<br>(Workflow mode only) | Click this button to approve the selected schedule. You are prompted for an optional comment to explain the approval, and an e-mail is generated to the approver and submitter in Workflow mode. |

| Element | Description |
|---|---|
| Discard button | Click this button to discard the selected schedule. You can discard a schedule unless there is an active deployment job that was created from the schedule. (You can wait for the job to finish, or abort the job and then discard the schedule.)<br>You are prompted for an optional comment to explain the discard, and an e-mail is generated to the approver and submitter in Workflow mode. |
| Refresh button | Click this button to reload schedule information from the Security Manager server. If the message *Auto Refresh is On* is displayed beneath the table, the schedule list is automatically refreshed periodically.<br>**Note** The auto refresh setting is configured in the administration settings for deployment: select **Tools > Security Manager Administration > Deployment**. |
| Suspend button | Click this button to suspend the selected schedule. Suspending the schedule does not delete the schedule, but it prevents the creation of deployment jobs based on it. You are prompted for a comment to explain the suspension, and an e-mail is generated to the approver in Workflow mode. |
| Resume button | Click this button to reactivate a suspended schedule. You are prompted for a comment to explain the suspension, and an e-mail is generated to the approver in Workflow mode. |
| Summary tab | Displays summary information about the selected schedule. Besides the fields shown in the table, summary information includes the number of devices included in the schedule and the user ID of the person who last changed the schedule. |
| Devices tab | Displays the devices that are included in the selected schedule. These are the devices to which configurations are deployed when a deployment job is created from the schedule. To change the device list, click **Open**, then click **Add Devices** on the Schedule dialog box. |
| History tab | Displays a log of the changes that have been made to the selected schedule. The information includes the state changes, the user who made the change, the date and time of the change (based on the Security Manager server time), and any comments the user entered to document the change. |
| Jobs tab | Displays a list of the deployment jobs that have been created based on the selected schedule. Information includes the name of the job, the date and time the job was created based on server time (not the client time), and the job status. If you select a job, and click the **Deployment Job** tab, the selected job is highlighted and you can view the job details.<br>For information on job status, see these topics:<br>• Job States in Workflow Mode , on page 7<br>• Job States in Non-Workflow Mode , on page 5 |

# Configuration Archive Window

The Configuration Archive stores configuration versions for each device managed by Security Manager. If you delete a device from Security Manager, all of the device's configurations are also deleted from the Configuration Archive.

You can use Configuration Archive to:

- View the transcript of a configuration deployment for a selected device.
- View and compare configuration versions.
- View CLI differences between deployed configuration versions.
- Roll back to an earlier configuration version, provided that the configuration originated from the device. You should roll back configurations only under extreme circumstances. For more information, see these topics:
  - Understanding Configuration Rollback , on page 65
  - Using Rollback to Deploy Archived Configurations , on page 73
- Add the current running configuration for a device to the archive.

You can sort the list of configuration versions for a device by clicking on the column heading that you want to sort on. Clicking the column heading toggles between sorting the rows in ascending or descending order. You can also control the fields displayed by right-clicking on any column heading and selecting or deselecting the desired column names under the Show Columns command.

### Navigation Path

Select **Manage > Configuration Archive**.

### Related Topics

- Configuration Archive Page
- Viewing and Comparing Archived Configuration Versions , on page 61
- Understanding Configuration Rollback , on page 65
- Using Rollback to Deploy Archived Configurations , on page 73
- Understanding Rollback for Devices in Multiple Context Mode , on page 66
- Understanding Rollback for Failover Devices , on page 67
- Understanding Rollback for Catalyst 6500/7600 Devices , on page 67
- Understanding Rollback for IPS and IOS IPS , on page 68
- Adding Configuration Versions from a Device to the Configuration Archive , on page 61
- Filtering Items in Selectors

## Field Reference

*Table 8: Configuration Archive Window*

| Element | Description |
|---|---|
| Device Selector | Lists the devices in the device inventory. Select a device to see the configuration versions for the device that are available in the archive. These are displayed in the right pane. |
| Version ID | The version number of the configuration version. By default, this column is not displayed. To display it, right click any column heading and select **Show Columns > Version ID**. |
| Created On | The date and time that the configuration version was archived. |
| Created By | The user ID or system ID associated with adding the configuration version to the archive.<br>If there are two names in the form *username1* (*username2* ), the first name is the user who initiated the request, and the name in parentheses is the system identity user. For more information on the system identity trust user, see the Installation Guide for Cisco Security Manager . |
| Archival Source | The origin of the archiving event (for example, User Request, Deployment or Provision, Discovery). |
| Creation Comment | A description about how or why the configuration version was created. |
| Transcript Icon | When double-clicked, displays a transcript of a configuration version that was deployed to a device.<br>A transcript is the log file of transactions between Security Manager and a device captured during a deployment or rollback operation. It includes commands sent and received between server and device from the time of the deployment or rollback request, but it does not include communication that occurs during the initial discovery phase of deployment, when Security Manager obtains the current configuration from the device. |
| View button | Click this button to display the selected configuration in the Config Version Viewer window (see Configuration Version Viewer , on page 62), where you can also compare the configuration to other configuration versions. |
| Rollback button | Click this button to roll the device configuration back to the selected configuration version, provided that the configuration originated from the device. You should roll back configurations only under extreme circumstances. For more information see these topics:<br>• Understanding Configuration Rollback , on page 65<br>• Using Rollback to Deploy Archived Configurations , on page 73 |

| Element | Description |
|---|---|
| Add from Device button | Click this button to have Security Manager retrieve the current running configuration from the device and add it as a configuration version to the archive. This is useful for any device whose configuration might have been changed directly in its CLI.<br>For more information on adding configuration versions, see Adding Configuration Versions from a Device to the Configuration Archive , on page 61. |

# Working with Deployment and the Configuration Archive

The following topics provide information about managing deployment and using the Configuration Archive:



## Viewing Deployment Status and History for Jobs and Schedules

Using the Deployment Manager, you can view status and history information for deployment jobs and schedules, as well as create and manage them. To open the Deployment Manager window, select **Manage > Deployments**.

Jobs and schedules are displayed on separate tabs. However, as jobs are created based on a deployment schedule, those jobs appear in the regular jobs list. Click the appropriate tab to view the list of jobs or schedules, where you can see this information:

- Deployment Jobs—The top pane displays a list of the deployment jobs. If you select a job, more detailed information appears in the lower pane:

- Summary tab—The Summary tab shows information such as the job status, number of devices deployed successfully, and number of devices deployed with errors.
- Details tab—The Details tab shows the status details for each device in the deployment.
- History tab (Workflow mode only)—The 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.

- Deployment Schedules—The top pane displays a list of the deployment schedules. If you select a schedule, more detailed information appears in the lower pane:
  - Summary tab—The Summary tab shows information such as the schedule, the time of the next job to be created from the schedule, the time a job was last run based on the schedule, the number of devices included in the schedule and the user ID of the person who last changed the schedule.
  - Devices tab—The Devices tab shows the list of devices that are included in the schedule.
  - History tab—The History tab shows the state changes and related comments of the schedule. You can track which user performed each action.
  - Jobs tab—The Jobs tab shows a list of deployment jobs that were created from the schedule and their statuses. You can also view these jobs on the Deployment Jobs tab.

The status information in the Deployment Manager window refreshes automatically unless you turned off automatic refresh in the Security Manager Administration Deployment page (Tools > Security Manager Administration > Deployment). A message below the job or schedule table indicates whether automatic refresh is on. If it is off, refresh status information by clicking **Refresh**.

### Related Topics


- Overview of the Deployment Process , on page 1
- Deploying Configurations in Non-Workflow Mode , on page 28
- Deploying a Deployment Job in Workflow Mode , on page 40
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42
- Deploying Configurations to a Token Management Server , on page 43
- Previewing Configurations , on page 44
- Redeploying Configurations to Devices , on page 54
- Aborting Deployment Jobs , on page 56
- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Creating or Editing Deployment Schedules , on page 56
- Suspending or Resuming Deployment Schedules , on page 60

# Tips for Successful Deployment Jobs

Successful deployment depends on many things, as explained in Troubleshooting Deployment. In addition to factors involving network communications and the proper functioning of the device, you can also improve the results of deployment by keeping the following tips in mind when you select devices for a deployment job or start the job:

- 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 and the device will be non-functional.
- Firewall devices only—If you manually added a firewall device (as described in Adding Devices by Manual Definition), 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 Default Firewall Configurations. For more information about importing policies, see Discovering Policies.
- Deployment might take from a few minutes to an hour or more, depending on the number of devices in the deployment job.
- Modifying a subset of devices that are part of a VPN might make the VPN inoperable. If you select a subset of devices that are part of a VPN when creating a deployment job, you are warned and given the opportunity to select the other devices in the VPN. See Warning - Partial VPN Deployment Dialog Box , on page 31.
- You cannot select devices that were included in other deployment jobs that are in an active state (Edit, Edit Open, and Approved). You can select devices that were included in other deployment jobs that are in the Deployed, Failed, Discarded, or Aborted states.
- Firewall service modules (FWSMs) and Intrusion Detection System service modules (IDSMs) contain virtual devices. Security Manager considers the module and the virtual devices to be separate devices.
- Some changes to the FWSM might require the Catalyst Multiservice function card (MSFC) to be updated as well. If you select an FWSM that has these types of changes, Security Manager notifies you that you must include the MSFC in the deployment job, and it will select the MSFC device for you automatically. However, if the MSFC is already included in another active deployment job, you cannot include the MSFC in the current deployment job. You must remove the MSFC from the other deployment job, discard the other deployment job, or include the FWSM in the other deployment job.
- 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.

### Related Topics


- Overview of the Deployment Process , on page 1
- Deploying Configurations in Non-Workflow Mode , on page 28
- Creating and Editing Deployment Jobs , on page 35
- Managing Device Communication Settings and Certificates
- Detecting and Analyzing Out of Band Changes , on page 46

- Job States in Non-Workflow Mode , on page 5
- Job States in Workflow Mode , on page 7

# 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 create them as configuration files in a directory on the Security Manager server. See Understanding Deployment Methods , on page 9 for more information.

**Note** If you have made changes to a Unified ACL entry through Policy Object Manager which is used in a RAVPN policy (DAP, Group Policy, and alike) on a device, the device and the ticket does not get displayed in the Deploy Saved Changes window. You must click Add other devices and add the device manually.

**Tip** Before creating the deployment job, read Tips for Successful Deployment Jobs , on page 27. That topic includes tips and cautions you should keep in mind when creating deployment jobs.

**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.

**Note** When using virtual sensors: An IPS device and all of the virtual sensors on it must be deployed as a group. If you make changes to a virtual sensor and then deploy it, Security Manager deploys the parent device and all virtual sensors associated with it.

### Before You Begin

- Make sure that devices have been bootstrapped. For more information, see Preparing Devices for Management.
- 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.

### Related Topics

- Overview of the Deployment Process , on page 1
- Including Devices in Deployment Jobs or Schedules , on page 8
- Understanding Deployment Methods , on page 9
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42
- Deploying Configurations to a Token Management Server , on page 43

- Managing Device Communication Settings and Certificates
- Understanding How Out-of-Band Changes are Handled , on page 12

**Step 1** Do one of the following in non-Workflow mode:

- Select **File > Submit and Deploy** or click the **Submit and Deploy Changes** button on the toolbar.

**Note** These options are not available when Ticket Management is enabled.

- Select **File > Deploy**.
- Click the **Deployment Manager** button on the Main toolbar and click the **Deployment Jobs** tab if it is not active. Click **Deploy**.

Security Manager validates all of the policy changes that were made since the last deployment. If the validation results in errors, resolve the errors before attempting to deploy again. If there are only warnings or informational messages, click **OK** to proceed to the Deploy Saved Changes dialog box.

**Step 2** In the Deploy Saved Changes dialog box, do the following:

- Select the devices to which you want to deploy configurations. The device selector lists all devices for which policy changes were made but not yet deployed, and initially all changed devices are selected for deployment.

All device groups that contain changed devices are shown, and you can select or deselect the devices using the device group folder. If you select or deselect a device that appears in more than one group, it is selected or deselected in all groups; however, a device is deployed to only once in the job. Right-click and select **Expand All** to open all of the folders.

The Deploy Saved Changes dialog box shows the date, time, and user associated with the changes that will be included in the deployment for the selected devices. This information changes based on the devices you select for deployment. If you have Ticket Management enabled, the tickets associated with the changes to be deployed are also displayed. You can click a ticket ID to view details of the ticket and to navigate to an external ticket management system if configured (see Ticket Management Page).

If you detect out of band changes, when you close the OOB Changes dialog box, the device names are color-coded based on the results: green indicates out of band change; red indicates an error during the detection process; no color change indicates no out of band changes.

- If you want to add devices that do not have policy changes to the deployment job, click **Add other devices** to open the Add Other Devices dialog box (see Add Other Devices Dialog Box , on page 59). You might want to add unchanged devices 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).
- (Optional) To change the method used to deploy configurations, click **Edit Deploy Method** to open the Edit Deployment Method dialog box (see Edit Deploy Method Dialog Box , on page 30). There is a system default deployment method (which your organization chooses), so you might not need to change the method. You can select these methods:
  - Device—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see Deploying Directly to a Device , on page 9 or Deploying to a Device through an Intermediate Server , on page 10.
  - File—Deploys the configuration file to a directory you select on the Security Manager server. For more information, see Deploying to a File , on page 11.

Before proceeding with the deployment, you can do the following:

- Preview proposed configurations and compare them against last deployed configurations or current running configurations. Right-click the device and select **Preview Config**. For more information, see Previewing Configurations , on page 44.
- Analyze the devices for out of band changes by clicking the **Detect OOB Changes** button. For more information, see Detecting and Analyzing Out of Band Changes , on page 46 and OOB (Out of Band) Changes Dialog Box , on page 49.

**Step 3** Click **Deploy** to start the deployment job for the selected devices, which generates the required configuration files and applies them according to your selected deployment method.

The Deployment Status Details dialog box opens so that you can view the status of the deployment. 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 , on page 32.

If deployment to any device failed, you can redeploy configurations to the failed devices. For more information, see Redeploying Configurations to Devices , on page 54.

## Edit Deploy Method Dialog Box

Use the Edit Deploy Method dialog box to specify whether to deploy the generated configurations directly to the devices in the network or to create configuration files in a directory on the Security Manager server.

### Navigation Path

Click **Edit Deploy Method** in the Deployment—Create or Edit a Job dialog box (Workflow mode) or Deploy Saved Changes dialog box (non-Workflow mode). For the procedures, see:

- Creating and Editing Deployment Jobs , on page 35
- Deploying Configurations in Non-Workflow Mode , on page 28

### Related Topics

- Understanding Deployment Methods , on page 9
- Deploying Configurations in Workflow Mode , on page 34
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42
- Deploying Configurations to a Token Management Server , on page 43
- Managing Device Communication Settings and Certificates

### Field Reference

*Table 9: Edit Deploy Method Dialog Box*

| Element | Description |
|---|---|
| Device | The name of the device. |
| Method | The deployment method to use:<br>• Device—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see Deploying Directly to a Device , on page 9 or Deploying to a Device through an Intermediate Server , on page 10.<br>• File—Deploys the configuration file to a directory on the Security Manager server. If you select File, specify the directory to which you want to deploy the configuration file in the Destination column. You cannot use file deployment with IPS devices. For more information, see Deploying to a File , on page 11.<br>**Note** To set the deployment method for more than one device at a time, select the desired rows, right-click and select **Edit Selected Deploy Method**. The Edit Selected Deploy Method dialog box opens where you can make your selections. |
| Destination | If you selected File in the Method field, enter the directory to which you want to deploy the configuration file. Click **Browse** to select from a list of available directories. |
| Preview Config button | Click this button to display the proposed configuration changes for the selected device. You can compare it to the last deployed configuration or the current running configuration. For more information, see Previewing Configurations , on page 44. |
| Out of Band Change Behavior | Click the radio button corresponding to the action you want Security Manager to take regarding changes made directly on the device using the CLI. For a complete explanation of how to handle out-of-band changes, including the meaning of the available options, see Understanding How Out-of-Band Changes are Handled , on page 12. |

## Warning - Partial VPN Deployment Dialog Box

Use the Partial VPN Deployment dialog box to select other devices that are part of a VPN to which you are deploying configurations.

When you create a deployment job and the job contains devices in a VPN, you must select all of the devices in the VPN. If you select a subset of devices and try to deploy to only those devices, this dialog box appears so that you can select the other devices that are part of the VPN.

### Navigation Path

- Non-Workflow mode—If you select a subset of devices in a VPN in the Deploy Saved Changes dialog box, this dialog box appears when you click **Deploy**.
- Workflow mode—If you select a subset of devices in a VPN in the Create or Edit a Job dialog box, this dialog box appears when you click **OK**.

### Related Topics

- Creating and Editing Deployment Jobs , on page 35
- Deploying Configurations in Non-Workflow Mode , on page 28
- Deploying Configurations in Workflow Mode , on page 34

### Field Reference

*Table 10: Partial VPN Deployment Warning Dialog Box*

| Element | Description |
|---|---|
| VPN | The name of the VPN. |
| Missing Devices | All the devices in the VPN that were not selected for deployment. |
| Is Device in Other Job | Whether the missing device is part of another deployment job. |
| Deploy to All Devices in VPN button | Click this button to deploy to all devices in the VPN.<br>You can deploy to all devices in the VPN only if the devices are not in other deployment jobs. |
| Deploy to Selected Devices button | Click this button to deploy only to the devices selected in the Create or Edit a Job or Deploy Saved Changes dialog boxes. |

## Deployment Status Details Dialog Box

The Deployment Status Details dialog box appears while configurations are being deployed to selected 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 for that device.

**Note** You can click **Close** to close this dialog box and continue working in Security Manager while deployment continues.

### Navigation Path

From the Deploy Saved Changes dialog box, click **Deploy**.

### Related Topics

- Overview of the Deployment Process , on page 1
- Deploying Configurations in Non-Workflow Mode , on page 28
- Tips for Successful Deployment Jobs , on page 27
- Managing Device Communication Settings and Certificates

- Device Communication Page

### Field Reference

***Table 11: Deployment Status Details Dialog Box***

| Element | Description |
|---|---|
| Deployment Status Details | |
| Progress Status Bar | A visual representation and percentage of devices that were successfully updated. |
| Status | The status of the deployment. The possible states are Deploying, Aborted, Successful, and Failed. For descriptions of these states, see Job States in Workflow Mode , on page 7. |
| Deployment Job Name | The name of the deployment job. |
| Devices To Be Deployed | The total number of devices in the deployment job. |
| Devices Deployed Successfully | The number of devices that were updated successfully. |
| Devices Deployed With Errors | The number of devices that failed to be updated. |
| **Deployment Details**<br>This table lists the devices that are included in the deployment job. | |
| Device | The name of the device. |
| Status | The status of the deployment to the device. For descriptions of these states, see Job States in Non-Workflow Mode , on page 5. |
| Summary | The number of warnings, errors, and failures for the device. |
| Method | The method of deployment to the device. Possible methods are File and Device. |
| Config | The device configuration file. Double click the icon to preview the configuration for a device. For more information, see Previewing Configurations , on page 44. |
| Transcript | The commands Security Manager issued to the device and the responses from the device during deployment if you are deploying to the device (instead of deploying to a file). Double-click the icon to see the transcript for a device. |
| Last Ticket(s) | The tickets containing changes that are part of the deployment for the device. You can click on the Ticket IDs to view additional information about the ticket, such as Creator and Last Modified date. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Device Communication Page). |

| Element | Description |
|---|---|
| Messages | The warning, error, and failure messages, as indicated by the severity icon.<br>When you select an item, the Description box to the right describes the message in detail. The Action box to the right provides information on how you can correct the problem. |
| Generate Report button | Click this button to create a deployment status report for this job. You can generate the report in HTML and PDF formats. The report includes a summary of the job plus the full and delta configurations and the job transcript. You can use this report for your own purposes or to aid in troubleshooting a problem with Cisco TAC. For more information, see Generating Deployment or Discovery Status Reports. |
| Refresh button | Click this button to update the status information. |
| Abort button | Click this button to abort the deployment job. 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. |

# Deploying Configurations in Workflow Mode

The task of deploying configurations in Workflow mode is a multiple step process. You must create a deployment job, get it approved, and then deploy the job. This process ensures that organizations that separate task authorizations among personnel can implement their control processes.

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 create them as configuration files in a directory on the Security Manager server. See Understanding Deployment Methods , on page 9 for more information.

**Tip** Before creating the deployment job, read Tips for Successful Deployment Jobs , on page 27. That topic includes tips and cautions you should keep in mind when creating deployment jobs.

### Before You Begin

- Make sure that devices have been bootstrapped. For more information, see Preparing Devices for Management.
- 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.

### Related Topics

- Overview of the Deployment Process , on page 1
- Including Devices in Deployment Jobs or Schedules , on page 8
- Understanding Deployment Methods , on page 9
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42

- Deploying Configurations to a Token Management Server , on page 43
- Managing Device Communication Settings and Certificates
- Understanding How Out-of-Band Changes are Handled , on page 12

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

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

**Step 2** Create the deployment job. Click **Create** and enter the job properties. For the procedure, see Creating and Editing Deployment Jobs , on page 35.

When you finish creating a job, you can select whether to submit it. If you are not using a deployment job approver, you can also automatically submit, approve, and deploy the job, in which case you do not need to complete the other steps in this procedure.

**Step 3** (Workflow with approver) Submit the job. If you did not submit the job, select it in the Deployment Manager window and click **Submit**. An e-mail is sent to the approver. For more information, see Submitting Deployment Jobs , on page 38.

**Step 4** (Workflow with or without an approver) Approve the job. If you did not approve the job when you created it, select it in the Deployment Manager window and click **Approve**. If there is a separate person who approves jobs, that person must perform this step. For more information, see Approving and Rejecting Deployment Jobs , on page 39.

**Step 5** (Workflow with or without an approver) Deploy the job. If you did not deploy the job when you created it, select it in the Deployment Manager window and click **Deploy**. You can specify a future time to start the job, or start it immediately, and configurations are deployed according to the properties of the job. For more information, see Deploying a Deployment Job in Workflow Mode , on page 40

**Note** You can discard a deployment job at any time before you deploy it. For more information, see Discarding Deployment Jobs , on page 41.

## Creating and Editing Deployment Jobs

In Workflow mode, before you deploy policy configurations to your devices, you must create a deployment job. When you create a job, you select 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.

**Note** If you have made changes to a Unified ACL entry through Policy Object Manager which is used in a RAVPN policy (DAP, Group Policy, and alike) on a device, the device and the ticket does not get displayed in the Deployment- Create a Job window. You must click Add other devices and add the device manually.

**Tip** Before creating the deployment job, read Tips for Successful Deployment Jobs , on page 27. That topic includes tips and cautions you should keep in mind when creating deployment jobs.

**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 Devices for Management.
- 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.

**Related Topics**

- Overview of the Deployment Process , on page 1
- Including Devices in Deployment Jobs or Schedules , on page 8
- Understanding Deployment Methods , on page 9
- Understanding How Out-of-Band Changes are Handled , on page 12
- Job States in Workflow Mode , on page 7

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

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

**Step 2** Do one of the following:

- Click **Create** to create a new job.
- Select an editable job and click **Open** to edit the job. You cannot edit a job that has already been deployed.

The Create a Job or Edit a Job dialog box opens.

**Step 3** In the dialog box, do the following to define the contents of the job:

- **Job Name and Description**—Keep the default job name or enter a more meaningful name. Because the job name enables you to distinguish one job from another, you should assign a name that reflects the contents of the job. You cannot change the name after you create the job. Optionally, enter a description of the job.
- Select the devices to which you want to deploy configurations. The device selector lists all devices for which policy changes were made but not yet deployed, and initially all changed devices are selected for deployment.

All device groups that contain changed devices are shown, and you can select or deselect the devices using the device group folder. If you select or deselect a device that appears in more than one group, it is selected or deselected in all groups; however, a device is deployed to only once in the job. Right-click and select **Expand All** to open all of the folders.

If you detect out of band changes, when you close the OOB Changes dialog box, the device names are color-coded based on the results: green indicates out of band change; red indicates an error during the detection process; no color change indicates no out of band changes.

- If you want to add devices that do not have policy changes to the deployment job, click **Add other devices** to open the Add Other Devices dialog box (see Add Other Devices Dialog Box , on page 59). You might want to add unchanged devices 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).
- (Optional) To change the method used to deploy configurations, click **Edit Deploy Method** to open the Edit Deployment Method dialog box (see Edit Deploy Method Dialog Box , on page 30). There is a system default deployment method (which your organization chooses), so you might not need to change the method. You can select these methods:
  - Device—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see Deploying Directly to a Device , on page 9 or Deploying to a Device through an Intermediate Server , on page 10.
  - File—Deploys the configuration file to a directory you select on the Security Manager server. For more information, see Deploying to a File , on page 11.

Before proceeding with the deployment, you can do the following:

- Preview proposed configurations and compare them against last deployed configurations or current running configurations. Right-click the device and select **Preview Config**. For more information, see Previewing Configurations , on page 44.
- Analyze the devices for out of band changes by clicking the **Detect OOB Changes** button. For more information, see Detecting and Analyzing Out of Band Changes , on page 46 and OOB (Out of Band) Changes Dialog Box , on page 49.

**Step 4** Select how you want the job handled when you close the dialog box. The options available to you depend on whether you are using Workflow mode with a deployment job approver:

- **Without an approver**—If you are not using a separate approver, you have these options:
  - **Close the job**—Close the job and leave it in the edit state. Select this option if you know you want to make additional modifications to the job.
  - **Approve the job**—Close the job and approve it but do not deploy it. Configure the following:
  - **Comments**—(Optional) Comments about the job approval.
  - **Submitter**—The e-mail address of the person submitting the job for approval. Notifications of job state changes are sent to this address, which is initially the e-mail address associated with the user account you used to log into Security Manager. Ensure that the address is the correct one so that you receive the notifications.
  - **Deploy the job**—Close the job, approve it, and deploy it. Configure the following:
  - **Options**—Whether to Deploy Now or Schedule. If you select Schedule, additional fields appear where you can specify the date and time when the job should be run. The time is in 24-hour format and is based on the time zone of the Security Manager server, which is not necessarily the same time zone that you are currently in. The target time must be at least five minutes in the future.
  - **Comments**—(Optional) Comments about the deployment job.
  - **Send Deployment Status Notification**—Whether Security Manager should send e-mail notifications whenever the job status changes.

If you select this option, enter the e-mail addresses of the people who should receive notifications in the Job Completion Recipients field. If you enter multiple addresses, separate them with commas. The field initially contains the default approver and your e-mail addresses.

- **With an approver**—If you are using a separate approver, you can configure the following options:
  - **Submit the job**—Whether to submit the job for approval. By default this check box is selected.
  - **Approver E-mail**—The e-mail address of the approver if you are submitting the job for approval. The default approver e-mail address is entered in the field, but you can change it.
  - **Comments**—(Optional) Comments you want to send to the approver, if any.
  - **Submitter E-mail**—The e-mail address of the submitter. The field initially contains the e-mail address associated with the user account you used to log in, but you can change it to another address.

**Step 5** Click **OK**.

Depending on your selection for how to handle the job, you might still need to submit, approve, and deploy the job. See these topics for more information:

- Submitting Deployment Jobs , on page 38
- Approving and Rejecting Deployment Jobs , on page 39
- Deploying a Deployment Job in Workflow Mode , on page 40

## 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. You do not submit jobs in this mode. For more information, see Approving and Rejecting Deployment Jobs , on page 39.

**Note** You enable and disable deployment job approval under Tools > Security Manager Administration > Workflow. For more information, see Workflow Page.

This procedure assumes that you already created the job. You can also submit the job when you create it by selecting the **Submit the job** checkbox in the Create a Job dialog box.

**Related Topics**

- Deployment Manager Window , on page 15
- Job States in Workflow Mode , on page 7

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

The Deployment Status window appears. Click the **Deployment Jobs** tab if it is not active.

**Step 2** Select the job to submit.

**Step 3** Click **Submit**.

The Submit Deployment Job dialog box opens.

**Step 4** Enter the following information:

- **Approver**—The e-mail address of the person to be notified of your submission. The default approver e-mail address is entered in the field, but you can change it.
- **Comment**—(Optional) Comments you want to send to the approver, if any.
- **Submitter**—The e-mail address of the person submitting the deployment job. The field initially contains the e-mail address associated with the username you used to log into Security Manager, but you can change it to another e-mail address.

**Step 5** Click **OK**.

The job status changes to Submitted. The approver must approve the job before you can deploy it.

## 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 and Editing Deployment Jobs , on page 35.

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 Workflow Page.

**Related Topics**

- Deployment Manager Window , on page 15
- Job States in Workflow Mode , on page 7

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

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

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

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

You are prompted for an optional comment for your action. The comments are preserved in the history for the job. After submitting your comment, an e-mail notification is sent (if e-mail notifications are configured) and the job status changes to Approved or Rejected, as appropriate. The job can now be deployed (see Deploying a Deployment Job in Workflow Mode , on page 40).

## Deploying a Deployment Job in Workflow Mode

When you work in Workflow mode, to deploy configurations to devices you must create a deployment job and have it approved. If you are working without a separate approver, you can approve and deploy the job yourself. Otherwise, you must submit it to an approver.

Deploying a deployment job in workflow mode simply starts a job. You cannot change the contents of a job during deployment.

**Note** Deployment might take from a few minutes to an hour or more, depending on the number of devices in the deployment job.

### Before You Begin

- Make sure that devices have been bootstrapped. For more information, see Preparing Devices for Management.
- 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 and Editing Deployment Jobs , on page 35.
- If using Workflow mode with a deployment job approver, submit the job. For more information, see Submitting Deployment Jobs , on page 38.
- Approve the job. For more information, see Approving and Rejecting Deployment Jobs , on page 39.

### Related Topics

- Overview of the Deployment Process , on page 1
- Deployment Manager Window , on page 15
- Including Devices in Deployment Jobs or Schedules , on page 8
- Understanding Deployment Methods , on page 9
- Managing Device Communication Settings and Certificates

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

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

**Step 2** Select the job to deploy.

**Step 3** Click **Deploy**.

The Deploy Job dialog box opens.

**Step 4** In the Deploy Job dialog box, make these selections:

- **Options**—How you want to run the job. Select **Schedule** to run the job at some point in the future. Select **Deploy Now** to run the job immediately. If you schedule the job for a future time, the changes deployed in the job are based on the changes that existed when the job was created, not when the job is run.

If you select Schedule, date and time fields appear.

- Click the calendar icon to pick the day on which to run the job.
- In the Time field, enter the time to start the job in 24-hour clock format. The time must be in time zone of the Security Manager server, which is not necessarily the same as your time zone. The time must be at least 5 minutes in the future.
- **Comments**—(Optional) An explanation of why you are deploying the job.
- **Require Deployment Status Notifications, Job Completion Recipients**— Whether Security Manager should send an e-mail when the job status changes.

If you elect to send status notifications, enter the recipient's e-mail address. The field initially contains the e-mail address associated with the user account you used to log in. You can enter multiple addresses by separating them with commas.

**Step 5** Click **OK**.

You are returned to the Deployment Manager window. The job status changes to Deploying. When the deployment is complete, the job status changes to Deployed.

## Discarding Deployment Jobs

In Workflow mode, 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.

**Related Topics**

- Deployment Manager Window , on page 15
- Job States in Workflow Mode , on page 7

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

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

**Step 2** Select the job to discard.

**Step 3** Click **Discard**. You are prompted for an optional comment to explain why you are discarding the job.

# Deploying Configurations Using an Auto Update Server or CNS Configuration Engine

If your organization uses Auto Update Server (AUS) or Cisco Networking Services (CNS) Configuration Engine to manage the deployment of configurations to your network devices, you can use these intermediate servers with Security Manager. To perform this type of deployment, you need to set up the device, the AUS or Configuration Engine, and Security Manager properly. This procedure explains the tasks that you need to perform.

**Tip** You cannot successfully deploy a configuration to AUS that requires Security Manager to download other files to the device. For example, some remote access VPN policies allow you to configure plug-ins, Secure Client, and Cisco Secure Desktop configurations. These files are not sent to AUS. Do not use AUS if you want to configure these types of policy.

**Related Topics**

- Overview of the Deployment Process , on page 1
- Preparing Devices for Management
- Including Devices in Deployment Jobs or Schedules , on page 8
- Understanding Deployment Methods , on page 9
- Managing Device Communication Settings and Certificates

**Step 1** Set up the AUS or Configuration Engine using the documentation for those products.

**Step 2** Configure the devices to use the server. The following topics describe the configuration steps depending on the type of server and the desired setup:

- Setting Up AUS on PIX Firewall and ASA Devices

**Step 3** When you add the device to Security Manager, select the AUS or Configuration Engine for the device if your chosen method allows it. If the AUS or Configuration Engine is not already defined in Security Manager, you can identify it to Security Manager as you add the network device. For detailed procedures, see these topics:

- Adding Devices from the Network
- Adding Devices from Configuration Files
- Adding Devices by Manual Definition
- Adding Devices from an Inventory File
- Adding, Editing, or Deleting Auto Update Servers or Configuration Engines

**Tip** After you add a device to the Security Manager inventory, you can change the assigned server in the device properties. Right-click the device and select **Device Properties**. Configure the server using the device properties if you could not identify it while adding the device.

**Step 4** For devices that are using AUS, configure the AUS policy for the device in Security Manager. Do one of the following:

- Configure the policy for a single device. In Device view, select the device, and then select **Platform > Device Admin > Server Access > AUS** from the Device Policy selector.
- Configure a shared policy that you can assign to many devices that share the same AUS. In 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 to change the policy. Select the Assignments tab to assign the policy to specific devices.

The server you identify in this policy must also be the server you identify in the device properties. The device properties identify the server to which Security Manager will send the configuration, whereas the AUS policy defines the server the device will contact.

**Tip** If you change AUS servers, keep in mind that the device will continue to use the AUS server defined in its current configuration until it receives a new configuration. Thus, you should change the AUS policy but deploy the configuration using the previous AUS server. After deployment is successful, change the device properties to point to the new server.

**Step 5** In Security Manager, deploy your configurations using the **Deploy to Device** deployment method. Security Manager sends the configuration to the AUS or Configuration Engine, where the network device retrieves it.

Depending on the Workflow mode you are using, follow these procedures:

- Deploying Configurations in Non-Workflow Mode , on page 28
- Deploying Configurations in Workflow Mode , on page 34

# Deploying Configurations to a Token Management Server

If your organization requires the use of a Token Management Server (TMS) for applying configuration updates to routers, you can use Security Manager in conjunction with your TMS processes. To perform this type of deployment, you need to set up the device, TMS, and Security Manager properly. This procedure explains the tasks that you need to perform.

**Related Topics**

- Overview of the Deployment Process , on page 1
- Preparing Devices for Management
- Including Devices in Deployment Jobs or Schedules , on page 8
- Understanding Deployment Methods , on page 9
- Managing Device Communication Settings and Certificates

**Step 1** Set up the TMS as an FTP server. Security Manager uses FTP to deploy the configuration file to the 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 the TMS product documentation for more information.

**Step 2** In Security Manager, select **Tools > Security Manager Administration > Token Management** to identify the TMS server to Security Manager.

By default, Security Manager uses the Security Manager server as the TMS, but you can specify a different server. You must enter the hostname or IP address, a username and password for the TMS, the directory to which configuration files should be copied, and the public key file location in Security Manager. For more information, see Ticket Management Page.

**Step 3** Specify TMS as the transport protocol to be used for Cisco IOS routers.

You can set this parameter globally for all Cisco IOS routers or for a specific device:

- Globally—Select **Tools > Security Manager Administration > Device Communication** and select TMS in **Transport Protocol (IOS Routers 12.3 and above)**.
- Device—Right click the device in the Device selector and select **Device Properties**. On the General tab, select TMS as the transport protocol in the Device Communications Group. Because not all routers support TMS, you might not be able to configure TMS for specific devices.

**Step 4** In Security Manager, deploy your configurations using the **Deploy to Device** deployment method. Security Manager sends the delta configuration to the TMS server.

Depending on the Workflow mode you are using, follow these procedures:

- Deploying Configurations in Non-Workflow Mode , on page 28
- Deploying Configurations in Workflow Mode , on page 34

**Step 5** Using the TMS, download the configuration to the eToken. See the TMS product documentation for more information.

**Step 6** Download the configuration from the eToken to the router and save the configuration to the device. Plug the eToken into the router, then enter the following commands to download the configuration to the router, where *usb_token_id* is either **usbtoken0** or **usbtoken1**, depending on which USB port you used. The default PIN is 1234567890.

**Example:**

```
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
```

**Tip** CCCD is the private sector on the eToken where the configuration file resides. When you enter the **crypto pki token default secondary config CCCD** command, the CLI on the e-token merges with the CLI on the router.

# Previewing Configurations

There are many ways to preview a device configuration. You can select a device from the Device selector and select **Tools > Preview Configuration**, or you can click the **Preview Config** button in several dialog boxes.

**Tip** You can also right click a device in Map view and select **Preview Configuration**.

When you preview a configuration, the configuration is displayed in the Config Version Viewer dialog box. The proposed configuration is on the left. You can select to view the delta configuration (which shows the changes since the last deployment) or the full configuration. You can also compare the configuration to the last one deployed to the device or the current running configuration in the right pane.

The contents of the proposed configuration can differ depending on where you view it from:

- If you use **Tools > Preview Configuration**, or right click the device in the Device selector and select **Preview Configuration**, the proposed configuration includes changes that you have not yet submitted to the database.
- If you preview the configuration while creating a deployment job, the proposed configuration includes only those changes that you have submitted to the database. These are the changes that will be deployed to the device if you start the deployment job.

The value of previewing configurations is that it lets you see the actual device commands that will be used to configure the device. If you are a CLI expert, this can help you verify that you are getting the configuration you expect. Even if you are not a CLI expert, you can use the information to look for more information in the command reference for the operating system on Cisco.com.

**Note** New objects are created when you rediscover ASA 8.2.3 devices through Cisco Security Manager after configuring network objects on the device. Ignore the CLIs for these new objects that are generated in preview configuration.

Following are some tips for previewing configurations:

- Many configuration options are specific to one or more interfaces. If you must specify an interface name in a policy, the previewed configuration will include the commands for the policy only if the Interfaces policy defines the interface that you specify. Ensure that you configure the Interfaces policy before previewing configurations.
- If you preview the configuration for a virtual sensor, the preview that you see is for the parent device, not the virtual sensor, because the configuration for a virtual sensor is stored on the parent device.
- If you are just curious about what commands a policy will configure, consider adding a dummy device and configure the policy for that device. This will help prevent unintended configuration changes in your real devices. To add a dummy device, use the procedure described in Adding Devices by Manual Definition.
- Policies are validated before you can view the configuration. The validation happens for all devices, not just the device you are previewing. Thus, you might see errors and warnings that apply to different devices. If any errors or warnings occur, the Preview Messages dialog box appears. The dialog box lists all of the messages, including their severity and possible solutions. Click **OK** to continue to the Config Version Viewer dialog box. Click **Details** to see detailed information on the problems.

The following table explains the fields in the Config Version Viewer window used for previewing configurations.

*Table 12: Config Version Viewer (Preview Configuration) Dialog Box*

| Element | Description |
|---|---|
| Proposed Config Type | The type of configuration you want to view. For example, you can view the full configuration or just the delta (the changes from the last deployed configuration). The proposed configuration is displayed in the left pane. |
| Compare to Version | Choose a configuration to compare against the proposed configuration. The selected configuration is displayed in the right pane.<br>• None—Leaves the reference configuration blank.<br>• Last Deployed—Displays the last configuration that was deployed to the device and compares it with the proposed configuration.<br>• Running Config—Displays the current configuration running on the device and compares it with the proposed configuration. The device must be accessible to obtain the running configuration. |
| First Difference button | Moves the cursor to the first difference noted between the proposed and reference configurations. |
| Previous Difference button | Moves the cursor to the previous difference noted between the proposed and reference configurations. |
| Current Difference button | Centers the currently selected difference on the page. |
| Next Difference button | Moves the cursor to the next difference noted between the proposed and reference configurations. |
| Last Difference button | Moves the cursor to the last difference noted between the proposed and reference configurations. |
| Print button | Prints the configuration. |

# Detecting and Analyzing Out of Band Changes

When you deploy configurations to devices, Security Manager either removes out of band changes or cancels the deployment based on your deployment settings. (For a detailed explanation of out of band changes and how they are handled during deployment, see Understanding How Out-of-Band Changes are Handled , on page 12.)

In the most typical scenario, Security Manager removes any out of band changes during deployment. However, there might have been good reason for those changes to have been made to the device outside of Security Manager. Thus, it is good practice to analyze a device for out of band changes before deploying configurations, so that you have the opportunity to proactively recreate any configuration changes that should be preserved.

**Note** When a device is rebooted from console, the Config_mod value becomes 0. Config_mod parameter value will be stored soon after a discovery or a deployment is done. Ideally, CSM will poll the device every 5 minutes to check for the config_mod parameter value changes to detect the OOB.

There are many ways to detect whether there have been out of band changes to a device configuration since the last deployment to the device. If there have been changes (by another device management application or by direct CLI updates), you can preview the changes and determine whether to update the device policies before deployment, or to deploy and overwrite those out of band changes. (Out of band changes are sometimes called OOB changes in Security Manager). In some scenarios, the OOB changes are not detected. For information on handling such exceptions, see Exceptions to Out of Band Change Detection, on page 48.

**Tip** Out of band change detection is available only for IOS, ASA, PIX, FWSM devices, and security contexts; it is not available for IPS devices. However, the settings for handling out of band changes during deployment also apply to IPS devices; the difference is that you cannot proactively analyze these changes in IPS devices prior to deployment.

To determine whether there have been out of band changes on one or more device, do any of the following in Device view:

- Select **Tools > Detect Out of Band Changes**. You are prompted to select the devices to evaluate for out of band changes. Select the devices or device groups, click >> to move them to the selected list, and click **OK**. For more information on selecting devices, see Using Selectors.
- Select one or more devices or device groups, right-click and select **Detect Out of Band Changes**. The selected devices are evaluated for changes.
- During deployment, select the devices to include in deployment and click the **Detect OOB Changes** button. (The button is available on the Deploy Saved Changes dialog box and the Deployment—Create or Edit a Job dialog box, depending on the workflow mode you are using.) The selected devices are evaluated for changes.

For information on the deployment procedure, see:

- Deploying Configurations in Non-Workflow Mode , on page 28
- Creating and Editing Deployment Jobs , on page 35

When you start the detection process, the OOB (Out of Band) Changes Dialog Box , on page 49 is opened so that you can view the results. Each selected device is evaluated by retrieving the current running configuration and comparing it to the most recent configuration stored in Configuration Archive. Security Manager does not consider any unmanaged policy types when evaluating differences between the configurations.

**Tip** Note that if you are in the process of deployment, the running configuration is **not** compared to the one you are proposing to deploy, so if you detect out of band changes, you might also want to preview the proposed configuration to see if you already implemented the same change in Security Manager policies. Right-click the device in the deployment dialog box and select **Preview Config**. You can compare the proposed configuration to the current running configuration. For more information, see Previewing Configurations , on page 44.

The OOB Changes dialog box shows the results of change detection. If a device has out of band changes, the icon for the device in the device selector changes to green. Select a device in the left pane of the OOB Detail tab to view the changes from the latest configuration in configuration archive. Use the buttons at the bottom of the window to move from change to change. The legend at the bottom explains the color coding used to describe the changes.

When evaluating changes, consider the following:

- If you want to keep the change, update the relevant policy in Security Manager to recreate the policy. Use preview config to ensure that your policy changes produce the desired results. Security Manager might use different naming conventions, so consider whether the policy results in the same thing, rather than being exactly the same text. Keep in mind that out of band change detection looks for syntactic differences, not semantic differences.
- If you use another application to configure certain types of policies, consider unmanaging that policy type in Security Manager. Security Manager ignores any configuration commands related to policies that it is not managing. For more information, see Policy Management Page.

**Note** A config_mod parameter value is stored whenever there is a device discovery or deployment. CSM polls every five minutes to check if the config_mod parameter value is changed and to detect the OOB changes. When you reload an ASA device from the console, the config_mod parameter value becomes 0 thus marking the OOB state in the device.

**Tip** If you are detecting changes during deployment, when you close the OOB Changes dialog box, the device names in the deployment dialog box are color-coded based on the results: green indicates out of band change; red indicates an error during the detection process; no color change indicates no out of band changes.

## Exceptions to Out of Band Change Detection

If you have not approved the activity in which the changes have been done, the Cisco Security Manager database will not get updated. This results in a discrepancy between the Cisco Security Manager configuration archive (that the OOB feature uses) and the Cisco Security Manager database. When you do not approve the activity, Cisco Security Manager does not detect Our of Band (OOB) changes that are applied to the device. As a result, Cisco Security Manager does not stop deployment (overwriting OOB changes) even when you have configured it to cancel deployment when OOB changes are detected (see Understanding How Out-of-Band Changes are Handled , on page 12). This section discusses this exception and how to handle it.

The following tasks are executed in Cisco Security Manager (Workflow mode), when a policy rediscovery is initiated:

**Step 1** After rediscovery (Discovering Policies on Devices Already in Security Manager), a new device configuration is written to the Cisco Security Manager configuration archive.

**Step 2** If you do not approve the activity in which policy rediscovery is done, the Cisco Security Manager database will not be updated with the new device configuration and will continue to use old configuration data. Thus, there will be a mismatch between the configuration archive and the Cisco Security Manager database. This might result in the OOB changes on the device to be overwritten by Cisco Security Manager. This occurs even when you have configured it to cancel deployment when OOB changes are detected (see Understanding How Out-of-Band Changes are Handled , on page 12).

**Note** If the policy rediscovery activity is not approved, Out of Band (OOB) changes are not detected between the Cisco Security Manager database and configuration on the device. This is because OOB changes are detected using the Cisco Security Manager configuration archive, which has been updated with discovered configuration from device (Step 1, on page 48 above). On the other hand, Cisco Security Manager database still has the previous configuration of device, since activity has not been approved.

### What to do next

In addition, when you are Previewing Configurations , on page 44 for the discovered device before the activity is approved, the preview configuration does not show correct configuration changes. In order to see correct differences, you must approve the activity first or preview configurations from another activity.

## Exceptions to Out of Band Change Detection

To overcome these exceptions, do the following:

**Step 1** Create a new activity for rediscovery.

**Step 2** On completion of policy rediscovery, Submit and Approve the activity. Verify if the activity has been approved.

**Step 3** To confirm if configuration changes for the rediscovered device is displayed as expected, perform Previewing Configurations , on page 44 for the device.

**Step 4** Deploy changes from Cisco Security Manager to the device, if required.

## OOB (Out of Band) Changes Dialog Box

Use the OOB Changes dialog box to view and analyze out of band changes on a device. An out of band change is any difference between the running configuration on a device and the most recent configuration for the device stored in Configuration Archive. Note that Security Manager considers only managed policy types when evaluating whether there is a difference between the configurations.

**Tip** Configurations are compared for syntactic differences, not semantic differences. Thus, functionally equivalent configurations might be identified as out of band changes.

**Tip** As an example, consider a simple case in which configuration lines are swapped in the device configuration without making any changes to the semantics. In this simple example case: 1) if there is an object group in Security Manager at line number 100, and 2) the same object group exists in the ASA configuration at any line number *except* 100, then 3) Security Manager detects and reports the change as OOB. To summarize this simple example case, Security Manager reports an OOB change even though this change in the order of a few configuration lines did not result in any changes to the semantics.

There are two tabs on this dialog box:

- **OOB Detail**—This tab shows the detailed results and progress of the detection process. The fields are described below.

- **OOB Summary**—This tab shows a summary of the detection results, and becomes available only after the detection process is completed on all selected devices. The information is by device and includes a time stamp (date, time, time zone) and difference data that indicates the additions, subtractions, and changes with the associated configuration line number. You can select text on this tab, use Ctrl+click to copy it to the clipboard, and paste it in another application (such as NotePad).

For more information on detecting and analyzing out of band changes, see Detecting and Analyzing Out of Band Changes , on page 46. For more information on handling out of band changes during deployment, see Understanding How Out-of-Band Changes are Handled , on page 12.

Beginning with Version 4.7, Security Manager has a tool to help you re-sync out of band changes. For more information on this new tool, see OOB Re-sync. Tool, on page 51

### Navigation Path

There are several ways to start the out of band change detection process. You can use the **Tools > Detect Out of Band Changes** command, or select one or more devices right-click and select **Detect Out of Band Changes**. You can also click the **Detect OOB Changes** button in Deploy Saved Changes dialog box and Deployment—Create or Edit a Job dialog box as explained in the following procedures:

- Deploying Configurations in Workflow Mode , on page 34
- Creating and Editing Deployment Jobs , on page 35

### Related Topics

- Previewing Configurations , on page 44
- Filtering Items in Selectors

### Field Reference

*Table 13: OOB Changes Dialog Box*

| Element | Description |
|---|---|
| Selected Devices list (left pane) | This list contains all devices you selected to evaluate for out of band changes, organized in device groups (if any).<br>Select a device to see the results in the right pane.<br>The icons for the devices change color based on the results of the detection process:<br>• Green—There are out of band changes.<br>• Red—The out of band detection process failed for some reason.<br>• No color change—No out of band changes. |

| Element | Description |
|---|---|
| Configuration Comparison (right pane) | The right pane shows the results of the change detection process for the selected device. Messages will indicate if OOB detection is still in progress, if there are no changes, or if there was an error that prevented change detection from completing.<br>If there are changes, the right pane shows both the running configuration retrieved from the device and the latest configuration for the device stored in Configuration Archive. The legend at the bottom of the window describes the color coding used to indicate changes, and you can use the following buttons to move from change to change. |
| First Difference button | Moves the cursor to the first difference noted between the configurations. |
| Previous Difference button | Moves the cursor to the previous difference noted between the configurations. |
| Current Difference button | Centers the currently selected difference on the page. |
| Next Difference button | Moves the cursor to the next difference noted between the configurations. |
| Last Difference button | Moves the cursor to the last difference noted between the configurations. |

## OOB Re-sync. Tool

The OOB Re-sync Tool, which is new in Security Manager 4.7, helps you re-sync, or reconcile, out of band data. The OOB Re-sync Tool is an extension of the OOB Detection Tool available in Security Manager 4.6 and earlier versions and continued into 4.7.

**Tip** Out of band (OOB) data is the difference between the last archived configuration of Security Manager and the latest configuration running on the device. OOB data comes into existence—with the result that you need to update the device CLI—for reasons such as these: 1) emergency requirements (primarily for ACLs) mean that there is no time to use Security Manager and complete its workflow process because an unknown validation error is blocking deployment; 2) the use of management applications other than Security Manager to manage the same devices; and 3) <100% feature support by Security Manager for ASAs means that some ASA features need to be managed by using the CLI. Any changes made to a device using a third-party tool together with any CLI changes made to a device sum up as OOB data.

The OOB Re-sync Tool aims to automate the process of bringing OOB data on a device into your Security Manager installation while retaining the policy structures that you previously established.

Without the OOB Re-sync Tool, Security Manager (versions 4.6 and earlier) has only the following administrative options when OOB data is detected during deployment:

- Warn and override the OOB changes (Default)—Cisco Security Manager detects for OOB changes during deployment, warns the user of the OOB changes but goes ahead and negates/wipes out the OOB changes.
- Stop deployment—Aborts the deployment when OOB changes are detected.
- Do not check for OOB changes—OOB changes are not even detected during deployment and are overridden on the device.

The following objects are supported by the OOB Re-sync Tool:

- Network Object/Object-Group(s)
- Security Group(s)
- Service Object Group(s)
- User Group(s)
- Time Range Object(s)

**Note** The OOB Re-sync Tool does not support OOB changes for routers.

The OOB Re-sync Tool does not re-sync all objects/ACLs. It re-syncs access rules and unified access rules; it does not, for example, re-sync IPv6 access rules. Note the details for policies in the following list:

- Access rules (unified) are supported
- IPv4 access rules are supported
- IPv6-only access rules are *not* supported
- Ethertype ACLs are *not* supported
- Standard ACLs are *not* supported

The OOB Re-sync Tool has a straightforward work flow:

1. Detect OOB changes by using one of the following methods to run the existing tool:
   - **Configuration Manager > Tools > Detect Out Of Band Changes**... .
   - **Configuration Manager** > [tool bar] > **Detect OOB Changes** icon
   - **Configuration Manager > Device View >** right-click a device > click **Detect Out Of Band Changes**.
   - In the Deploy Saved Changes dialog box, click **Detect OOB**.
2. If out of band changes are detected, they appear in the right pane of the OOB (Out of Band) Changes Dialog Box on the OOB Details tab. The OOB Details tab displays a report of the changes and the target rule number, shared policy, sections, affected devices, and CLI.

   Also if out of band changes are detected, the Re-Sync Summary tab in the right pane of the OOB (Out of Band) Changes Dialog Box becomes active.

   After OOB changes are detected by the existing OOB detection tool, click Evaluate; after you do, Security Manager will further analyze the differences in the configuration running on the device and the configuration available in Security Manager. After this analysis, the Re-Sync Summary Tab becomes active. On this tab, Security Manager displays other details, such as ACE, object(s) that will be added or deleted, and rule location(s).

**Note** Security Manager also will annotate the policy rule table, both in Device and Policy View and for objects in the Policy Object Manager.

3. After the Re-Sync Summary Tab becomes active, you have the option of generating a report and checking to see if there is any CLI that is not supported by OOB functionality. After checking the report, you can opt to accept the changes by clicking **Accept**, and if the operation of persisting ACL or object changes in the device went through fine, you will be prompted with a "success" message.

**Note** If you modify access rules that are part of a shared policy, the OOB Re-sync Tool in this particular case will annotate both the rule that has actually been modified and the rule just above it. This occurs when you 1) modify at least two access rules that are part of a shared policy; 2) run the OOB Re-sync Tool; and 3) accept the changes. In this case, the OOB Re-sync Tool reports an OOB condition for some rules in addition to the ones that you modified. It is important to understand that the rules themselves and the shared policy are not adversely affected.

4. On the OOB Detail tab in the left pane, you can request a report in .pdf format. To do this click the **Generate Report** button. Cisco recommends that you always generate this report and save it to help with troubleshooting if needed.

**Tip** The following example is a brief description of a scenario in which you use the OOB Re-sync Tool and find some changes in a device that are not supported by the OOB Re-sync Tool along with access-rule changes that are supported. In this scenario, you have an ASA that uses both IPv4 and IPv6. If you use **Tools > Detect Out Of Band Changes..** and find OOB changes, you will need to manually reconcile the IPv6 changes before you can elect to re-sync. the OOB changes by using the OOB Re-sync Tool.

You should be aware of several caveats when using the OOB Re-sync Tool. These are listed in the following table.

***Table 14: Caveats***

| | |
|---|---|
| Interface Role | Access rules tied to interface roles and multiple interfaces rules will not be absorbed. However, the rules will be annotated to help the user copy the OOB rules from the OOB re-sync report and run "Import Rules" at the right rule location to absorb the OOB CLIs. |
| Shared Policies | OOB changes that affect shared policies will not be re-synced since doing so would affect other devices. Rules will be annotated to help the user import rules. |
| Objects | The OOB re-sync process always creates overrides for objects. However, if object override is selectively disabled for that object, then re-sync will not be allowed until the user enables the device overrides for that object. |
| Unsupported Access List | IPv6 only access-list that existed before the introduction of unified access-list is not supported for resync<br>Ether Type Access List re-sync is not supported |

| | |
|---|---|
| OOB Access-Group CLI | OOB changes on access-group CLI cannot be absorbed. To explain this caveat further:<br>• Under these circumstances (OOB changes on access-group CLI), you cannot choose evaluation; that is, you cannot elect to re-sync. the OOB changes.<br>• In a case involving both 1) OOB changes that the OOB Re-sync Tool can re-sync and 2) changes in access-group CLIs, you must resolve the changes with respect to the access-group command before you can elect to re-sync the OOB changes. |
| Conditional Re-sync of Remarks | ACL remarks added to an access-list CLI created out-of-band will be absorbed during re-sync as part of re-sync of the rule. However, any random OOB change in an ACL remark alone will not be absorbed during re-sync |
| Rule Split | Rules get split during re-sync of OOB changes done within combined rules. User needs to run "Combine Rules" on the flattened rules thus re-synced to restore to the original rule if possible |

### Related Topics

- Detecting and Analyzing Out of Band Changes , on page 46
- Understanding How Out-of-Band Changes are Handled , on page 12

# Redeploying Configurations to Devices

You can redeploy a deployment job if you want to. This is especially valuable for jobs in the Failed or Aborted states. You can redeploy to all devices in the job, or you can select specific devices (such as the devices to which deployment failed).

### Tips on Redeploying a Configuration to a Replacement Device

If you have to replace a device, for example, due to hardware failure, you cannot simply redeploy the last deployment job from the device, because Security Manager does not know that the device is actually a new one. To deploy the old device's configuration to the new device, you have these options:

- If the new device is the exact same model and operating system version as the replaced device, you can select the old device in the device selector, right-click and select **Preview Configuration**, and copy and paste the full configuration to the new device. However, this does not migrate certificates from the old device to the new one. You must re-enroll the device or renew the certificate yourself.
- If the new device is not exactly identical to the old device, follow the procedure described in Changes That Change the Feature Set in Security Manager.

### Before You Begin

- Make sure that devices have been bootstrapped. For more information, see Preparing Devices for Management.
- 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.

### Related Topics

- Overview of the Deployment Process , on page 1
- Deploying Configurations in Non-Workflow Mode , on page 28
- Deploying Configurations in Workflow Mode , on page 34
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine , on page 42
- Deploying Configurations to a Token Management Server , on page 43
- Managing Device Communication Settings and Certificates
- Understanding Deployment Methods , on page 9
- Job States in Non-Workflow Mode , on page 5
- Job States in Workflow Mode , on page 7

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

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

**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 opens. The dialog box lists the devices in the deployment job, showing the device name, the deployment method used, the status of the previous deployment, and the name of the deployment job that updated the device.

**Step 3** In the Redeploy a Job dialog box, do the following:

- **Selection column**—Select the devices to which you want to redeploy configurations by putting checkmarks in the checkboxes in the Selection column. Initially all failed devices are selected.
- **Deployment Method, Destination**—(Optional) You can change the method used to deploy configurations for individual devices. The initially selected method is the one used in the job. You can select these methods:
  - **Device**—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see Deploying Directly to a Device , on page 9 or Deploying to a Device through an Intermediate Server , on page 10.
  - **File**—Deploys the configuration file to a directory on the Security Manager server. If you select File, specify the directory to which you want to deploy the configuration file in the Destination column. Click **Browse** to select from a list of available directories. You cannot use file deployment with IPS devices. For more information, see Deploying to a File , on page 11.

**Note** To set the deployment method for more than one device at a time, select the devices, right-click and select **Edit Selected Deploy Method**. The Edit Selected Deploy Method dialog box opens where you can make your selections.

- **Out of Band Change Behavior**—(Optional) Select how you want Security Manager to respond if it detects that changes were made on the device by someone other than Security Manager (these are called out of band changes).

For a complete explanation of how to handle out-of-band changes, including the meaning of the available options, see Understanding How Out-of-Band Changes are Handled , on page 12.

**Note** Before proceeding with the deployment, you can preview proposed configurations and compare them against last deployed configurations or current running configurations. Highlight the row for a device and click **Preview Config**. For more information, see Previewing Configurations , on page 44.

**Step 4** Click **OK**.

# Aborting Deployment Jobs

You can stop a deployment job if you do not want to deploy the configurations 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 configurations 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.

To abort a job, do either of the following:

- Click Abort on the Deployment Status dialog box while you are viewing the running status of an active job. See Deployment Status Details Dialog Box , on page 32.
- Select **Manage** > **Deployments** to open the Deployment Manager window, then select the job on the Deployment Jobs tab and click **Abort**.

The Abort the Job dialog box opens and asks you to confirm that you want to abort the job. Click **OK** to confirm.

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 , on page 54 for more information.

### Related Topics

- Viewing Deployment Status and History for Jobs and Schedules , on page 25
- Job States in Non-Workflow Mode , on page 5
- Job States in Workflow Mode , on page 7

# Creating or Editing Deployment Schedules

You can create deployment schedules to create deployment jobs at regular intervals. Schedules can help you ensure that the selected devices get regular configuration updates.

**Tip** When you include a device in a schedule, the device is included in deployment jobs that are generated from the schedule only if changes have been made to the device configuration and those changes were committed to the database. Thus, you might see changes when previewing the device configuration even though the device was not included in a scheduled deployment, if you have not submitted those changes (or if they have been submitted by not yet approved, when using a separate approver in Workflow mode).

**Related Topics**

- Overview of the Deployment Process , on page 1
- Viewing Deployment Status and History for Jobs and Schedules , on page 25
- Suspending or Resuming Deployment Schedules , on page 60

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

The Deployment Manager window appears. Click the **Deployment Schedules** tab if it is not active (see Deployment Schedules Tab, Deployment Manager , on page 20).

**Step 2** Do one of the following:

- If you are creating a new schedule, click **Create**.
- If you are editing an existing schedule, select it in the Deployment Schedule table and click **Open**.

The Schedule dialog box opens (see Schedule Dialog Box , on page 58).

**Step 3** Enter at least this information in the Schedule dialog box:

- The name of the schedule.
- If you are using Workflow mode with an approver, ensure that the approver e-mail address is correct. Also verify your e-mail address (in the Submitter field), and choose whether you want to get notifications whenever the status of the job changes.
- Define the first date and time the schedule should start, and select how often deployment jobs will be generated based on the schedule. Also determine whether the schedule should have an end date, after which no new jobs are created from it.
- Click **Add Devices** and select all the devices that should be included in the deployment job. Including devices does not lock them from being modified by users or included in other deployment jobs or schedules.

If Security Manager is configured to use user-login credentials for accessing devices, your username and password are captured during schedule creation. If you change your password, you will need to recreate the schedule.

**Step 4** Click **OK**. The schedule is added to the Deployment Schedule table.

**Step 5** (Workflow mode only) If you are operating in Workflow mode, you must complete these additional steps:

- If you are using an approver for deployment jobs, select the schedule in the table and click **Submit** to submit the schedule to the approver. You are prompted to verify the approver's e-mail address and to enter comments to help the approver evaluate the schedule. The approver will have to approve the schedule before it becomes active.

- If you are not using an approver, select the schedule in the table and click **Approve** to approve it yourself and to activate the schedule.

# Schedule Dialog Box

Use the Schedule dialog box to create a regularly recurring deployment job.

### Navigation Path

Select **Manage** > **Deployments** to open the Deployment Manager window, click the Deployment Schedules tab in the upper pane, and do one of the following:

- Click **Create** to create a new schedule.
- Select a schedule and click **Open** to view or modify its properties.

### Related Topics

- Creating or Editing Deployment Schedules , on page 56
- Suspending or Resuming Deployment Schedules , on page 60

### Field Reference

*Table 15: Schedule Dialog Box*

| Element | Description |
|---|---|
| **Schedule Name Group**<br>This group defines the name of the job and the job's notification requirements. | |
| Name | The name of the job. When individual deployment jobs are created from this schedule, a time stamp is added to the job name. |
| Description | The description of the purpose of the job. |
| Approver Email<br>(Workflow only) | The e-mail address of the person who should approve the schedule. |
| Comments<br>(Workflow only) | (Optional) Information to help the approver evaluate the schedule when you save this schedule. |
| Submitter Email<br>(Workflow only) | The e-mail address of the person who is submitting this schedule for approval. This field initially contains the e-mail address associated with the user account you used to log into Security Manager, but you can change it. |

| Element | Description |
|---|---|
| Require Deployment Status Notifications<br>(Workflow only) | Whether to send e-mail messages for any change in the job status for the job schedule or any job created from it. Messages are sent to the approver and the submitter. |
| **Recurrence Pattern Group**<br>The fields in this group define the job schedule. | |
| Start Date | The first day of the schedule. Click the calendar icon to select the date from a calendar. |
| Time (Start) | The time of day to run the schedule. The time is in 24-hour format and is based on the server time zone, not the client time zone. |
| Recurrence | How often to create a deployment job based on this schedule:<br>• One time—Run this job once on the day specified as the start date at the specified start time.<br>• Hourly—Run this job on an hourly schedule. Specify the number of hours between deployment jobs.<br>• Daily—Run this job on a daily schedule. Specify the number of days between deployment jobs.<br>• Weekly—Run this job on the specified days of the week.<br>• Monthly—Run this job on a monthly schedule. Select the day of the month to run the job, and the number of months between deployment jobs. |
| Run Indefinitely<br>End Date and Time | The expiration date and time for the schedule. Deployment jobs are not created after this time. Select Run Indefinitely if you do not want the schedule to expire. |
| **Devices To Deploy Group**<br>This table lists the devices that are included in the deployment job. To add devices to the list, or to remove them from it, click **Add devices**, which opens the Add Other Devices dialog box (see Add Other Devices Dialog Box , on page 59.<br>If Security Manager is configured to use user-login credentials for accessing devices, your username and password are captured during schedule creation. If you change your password, you will need to recreate the schedule. | |

## Add Other Devices Dialog Box

Use the Add Other Devices dialog box to select devices for the deployment job or schedule. The devices in the list might not have active policy changes. When you are creating a job, you might want to add devices that do not have policy changes if a device was manually modified and you want to return the device to its previous configuration (the configuration stored in the Security Manager database).

- Select the devices to include in the job or schedule in the Available Devices list and click >> to move the devices to the Selected Devices list.
- To remove devices, select them in the Selected Devices list and click <<.

### Navigation Path

To open this dialog box, do one of the following:

- (Non-Workflow mode) From the Deploy Saved Changes dialog box, click **Add other devices**. See Deploying Configurations in Non-Workflow Mode , on page 28.
- (Workflow mode) From the Deployment—Create or Edit a Job Dialog Box, click **Add other devices**. See Creating and Editing Deployment Jobs , on page 35.
- (All modes) From the Schedule Dialog Box , on page 58, click **Add devices**.

### Related Topics

- Including Devices in Deployment Jobs or Schedules , on page 8
- Creating or Editing Deployment Schedules , on page 56
- Filtering Items in Selectors>

# Suspending or Resuming Deployment Schedules

You can suspend an active deployment schedule without discarding it and then reactivate it later when you want to resume creating jobs based on the schedule. This allows you to turn off a schedule temporarily.

### Related Topics

- Viewing Deployment Status and History for Jobs and Schedules , on page 25
- Creating or Editing Deployment Schedules , on page 56

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

The Deployment Manager window appears. Click the **Deployment Schedules** tab if it is not active (see Deployment Schedules Tab, Deployment Manager , on page 20).

**Step 2** Do one of the following:

- To suspend an active schedule, select it and click **Suspend**.
- To resume a suspended schedule, select it and click **Resume**.

# Adding Configuration Versions from a Device to the Configuration Archive

The Configuration Archive is updated with a new configuration version any time a configuration is deployed to the device or a file, including when you roll back a configuration to a device.

You can also retrieve a configuration directly from the device to add to the Configuration Archive. This is useful when changes have been made directly to device configurations, which are called out-of-band changes.

**Note** You cannot retrieve configurations from devices that are managed by AUS and that have been configured with dynamic IP addresses.

This procedure will help you retrieve a configuration from a device and add it to the archive.

**Related Topics**

- Viewing and Comparing Archived Configuration Versions , on page 61

**Step 1** Select **Manage > Configuration Archive** to open the Configuration Archive (see Configuration Archive Window , on page 23).

**Step 2** In the Device selector, select the device from which you want to retrieve the configuration. The archived configurations appear in the right pane.

**Step 3** Click **Add from Device**. Security Manager logs into the device, retrieves the running configuration, and adds it to the archive.

# Viewing and Comparing Archived Configuration Versions

Using the Configuration Archive, you can view the previous configurations for a device, compare versions of the configuration, and view the transcripts related to configuration deployment. To open the Configuration Archive window, select **Manage > Configuration Archive**.

To view the configuration versions for a device, select the device in the device selector. All archived versions are listed in the right pane. You can do the following:

- To view a configuration, select it and click **View**, which opens the Config Version Viewer dialog box with the configuration displayed in the left pane (for information about the dialog box, see Configuration Version Viewer , on page 62).

If there is more than one type of configuration available for the selected version, you can choose which type to view using the **Config Type** field. A Full version is a complete configuration, whereas a Delta version is just the commands that were different between this version and the device's previous full configuration. Delta configurations might include negative commands.

- To compare configurations, select one and click **View**. In the Config Version Viewer window, select the configuration you want to compare in the **Compare with Version** field. The second version appears in the right pane with differences color-coded according to the caption below the display area.
- To view the transcript associated with the deployment of a configuration, do one of the following:

- From the Configuration Archive window, double-click the icon in the Transcript column for the desired configuration.
- When viewing a configuration in the left pane of the Config Version Viewer dialog box, click **Transcript View**.

A transcript is the log file of transactions between Security Manager and a device captured during a deployment or rollback operation. It includes commands sent and received between server and device from the time of the deployment or rollback request, but it does not include communication that occurs during the initial discovery phase of deployment, when Security Manager obtains the current configuration from the device. If rollback is unsuccessful, there might be a partial transcript generated depending on which stage rollback or deployment failed. The transcript is displayed in the Transcript Viewer window (see Viewing Deployment Transcripts , on page 64).

You can configure the number of configuration versions to archive on the Configuration Archive settings page (see Configuration Archive Page).

### Related Topics

- Adding Configuration Versions from a Device to the Configuration Archive , on page 61

## Configuration Version Viewer

Use the Config Version Viewer window (when opened from the Configuration Archive) to view previous configurations for a device and to compare them to other archived configurations. You can compare any version to any other version in the archive for a selected device. The selected version appears in the left pane, and you can select another version for comparison from the list on the upper right of this window. For more information on viewing and comparing versions, see Viewing and Comparing Archived Configuration Versions , on page 61.

### Navigation Path

Select **Manage** > **Configuration Archive**, select a device whose configuration you want to view, select the configuration, and click **View**.

### Related Topics

- Configuration Archive Window , on page 23
- Viewing Deployment Transcripts , on page 64
- Viewing and Comparing Archived Configuration Versions , on page 61
- Adding Configuration Versions from a Device to the Configuration Archive , on page 61

### Field Reference

*Table 16: Configuration Version Viewer Window (Configuration Archive)*

| Element | Description |
|---|---|
| Version ID | The configuration version to display in the left pane:<br>• Previous—Display the version in the sequence before the one currently selected.<br>• Next—Display the version in the sequence after the one currently selected.<br>• Last—Display the last version in the list.<br>• Specific Date and Time—Display the version created on that date and time. |
| Compare with version | The configuration version to compare to the version selected in the left pane, if you want to compare versions. The configuration is displayed in the right pane, with differences summarized and color coded as explained by the caption below the pane. |
| Config Type | The types of configurations that are available for viewing. The types differ based on the type of device. The types might indicate Full or Delta, which have the following meaning:<br>• Full Configuration—The full configuration for the selected device as saved in the Configuration Archive. You can compare full configurations for a device.<br>• Delta Configuration—The file that is generated by Security Manager during deployment and that represents policy changes between the configuration selected in the Version ID field and the most recently deployed version.<br>**Note** Configuration versions resulting from out-of-band changes (for example, in the CLI) can be added to Configuration Archive using **Add from Device**, but no delta configuration file is generated. |
| First Difference button | Moves the cursor to the first difference noted between the configuration versions. |
| Previous Difference button | Moves the cursor to the previous difference noted between the configuration versions. |
| Current Difference button | Using the cursor, focuses on the currently selected difference in the window. |
| Next Difference button | Moves the cursor to the next difference noted between the configuration versions. |
| Last Difference button | Moves the cursor to the last difference noted between the configuration versions. |
| Transcript View button | Click this button to open the transcript viewer window, which displays the device communication transcript associated with this configuration. |
| Print button | Click this button to print the configuration. |

# Viewing Deployment Transcripts

Use the Transcript Viewer window to view the record of messages exchanged between Security Manager and a device. A transcript is the log file of transactions between Security Manager and a device captured during a deployment or rollback operation. It includes commands sent and received between server and device from the time of the deployment or rollback request, but it does not include communication that occurs during the initial discovery phase of deployment, when Security Manager obtains the current configuration from the device. For more information, see Viewing and Comparing Archived Configuration Versions , on page 61.

### Navigation Path

- Configuration Archive—Select **Manage > Configuration Archive** to open the Configuration Archive, select the device for which you want to view a transcript and double-click the **Transcript** icon in the row for the desired configuration version.

You can also click the **Transcript View** button from the Configuration Version Viewer window when examining an archived configuration (see Configuration Version Viewer , on page 62).

- Deployment Manager—Select **Manage > Deployments** to open the Deployment Manager, select the deployment job that includes the desired device deployment, select the Details tab in the lower pane, and double-click the **Transcript** icon in the row for the desired device.

### Related Topics

- Configuration Archive Window , on page 23
- Deployment Manager Window , on page 15

### Field Reference

*Table 17: Transcript Viewer Window*

| Element | Description |
|---|---|
| Version ID | The configuration version for which you are viewing transcripts:<br>• Previous—Display the transcripts for the version in the sequence before the one currently selected.<br>• Next—Display the transcripts for the version in the sequence after the one currently selected.<br>• Last—Display the transcripts for the last version in the list.<br>• Specific Date and Time—Display the transcripts for the version created on that date and time. |
| Transcript Type | The type of transcript that you want to view. Some configuration versions have more than one transcript associated with them. Use this field to select which transcript to view. |
| Transcript Window | Displays the selected transcript. You can select text and copy it to the clipboard (Ctrl+C) for pasting in a text editor. |

| Element | Description |
|---|---|
| View button | Click this button to display the related configuration in the Config Version Viewer window (see Configuration Version Viewer , on page 62). |
| Print button | Click this button to print the transcript. |

# Rolling Back Configurations

After you deploy a new configuration to a device, you can roll back the configuration to an older version if you find that the new configuration does not work correctly. However, it is usually a better idea to fix the configuration in Security Manager and deploy the fixed configuration, because rolling back a configuration creates a situation where the configuration defined in Security Manager is not the same one running on the device. Roll back configurations only in extreme circumstances.

The following topics will help you better understand and use configuration rollback:


- Understanding Configuration Rollback , on page 65
- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73
- Performing Rollback When Deploying to a File , on page 74


## Understanding Configuration Rollback

If you deploy configurations to devices using the Device method, either to deploy the configuration directly to the device or to an intermediate server, you can roll back the configuration to an older version if you find that the new configuration does not work correctly. You cannot roll back to a configuration that was deployed to a file.

**Caution** The Security Manager will take the device's current configuration after each deployment and save it in the configuration archive. When a device is rolled back, Security Manager pulls the previous configuration from the configuration archive and applies it to the device. The complete device configuration is used in this rollback procedure, making it an unreliable operation. We recommend you to use this operation only during extreme circumstances. It is usually a better idea to fix the configuration in Security Manager and deploy the fixed configuration, because rolling back a configuration creates a situation where the configuration defined in Security Manager is not the same one running on the device. After rollback, you should rediscover policies on the device to make the device configuration and its configuration in Security Manager consistent.

You can roll back configurations using these tools:

- Deployment Manager—You can roll back a deployment to the last good configuration if that configuration was deployed to the device rather than to a file. To open the Deployment Manager, select **Manage > Deployments**.
- Configuration Archive—You can roll back deployment to any archived configuration that was deployed to the device or that originated from the device. To open the Configuration Archive, select **Manage > Configuration Archive**.

When you roll back a configuration, Security Manager does the following:

- On PIX Firewalls and ASA and 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).
- For devices running IOS 12.3(7)T or later, Security Manager uses the **configure replace** command to replace the running configuration with the contents of a configuration file. Support for this command is dependent on the IOS version installed on the device:
  - On devices 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. 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, which restarts the system. Security Manager uses the TFTP server and directory specified in the Configuration Archive settings page (see Configuration Archive Page) when using this method.
- The rolled-back configuration becomes another archived version in the Configuration Archive for that device.

**Tip** Configuration rollback does not include user account policies. When you roll back a configuration, the existing state of user accounts is not changed. This helps ensure that users can continue to log into the device.

Special considerations apply to the rollback of certain device types and configurations. See the following sections for more information:

- Understanding Rollback for Devices in Multiple Context Mode , on page 66
- Understanding Rollback for Failover Devices , on page 67
- Understanding Rollback for Catalyst 6500/7600 Devices , on page 67
- Understanding Rollback for IPS and IOS IPS , on page 68
- Commands that Can Cause Conflicts after Rollback , on page 70
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73

## Understanding Rollback for Devices in Multiple Context Mode

If the configuration of the system execution space to which you are rolling back specifies connectivity options to security contexts (for example, vlan config) and there is a mismatch between the configuration selected for rollback and the current running configurations of the security contexts, Security Manager might not be able

to connect to the security contexts. In such cases. we recommend that you roll back configurations for the security contexts before rolling back a configuration for the system execution space.

If you roll back a configuration for the system execution space of a device in multiple context mode to one that includes a different set of security contexts, after rollback the security contexts on the device might not match the security contexts managed by Security Manager that appear in the Device selector.

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73
- Commands that Can Cause Conflicts after Rollback , on page 70
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

## Understanding Rollback for Failover Devices

If you roll back a configuration for a security context that contains a failover policy, Security Manager initially disables failover in the system execution space and both devices become active. After the rollback is completed, the devices should return to their failover configuration.

If a switchover occurs during rollback or connectivity between the active and standby units is lost, copy the bootstrap configuration to the standby unit after rollback completes. For more information, see Bootstrap Configuration for LAN Failover Dialog Box.

Security Manager can proceed with rollback action if and only if the following conditions are met:

- Both the Primary unit and Secondary unit must be in Active state.
- If configured on a link, the link must be up.
- If configured on LAN, the interface must be up.

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73
- Commands that Can Cause Conflicts after Rollback , on page 70
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

## Understanding Rollback for Catalyst 6500/7600 Devices

If you roll back a configuration to a Catalyst 6500/7600 device that specifies connectivity options to service modules (for example, vlan config) and there is a mismatch between the configuration selected for rollback and the current running configuration, Security Manager might not be able to connect to the service modules. We recommend that you roll back configurations for the service modules before rolling back a configuration to the Catalyst 6500/7600 chassis.

Thus, the proper order for performing rollback on Catalyst 6500/7600 devices is:

1. Security contexts.

2. Service modules.
3. Chassis.

We recommend performing rediscovery after the rollback operation is complete.

If you are rolling back an FWSM deployment and the system is configured to retrieve security certificates when adding devices, you might need to retrieve the certificate after the rollback operation is complete. This can be done using either of the following methods:

- Retrieving the certificate on a per-device basis from Device Properties.
- Configuring Security Manager to automatically retrieve certificates after rollback. To do this, select **Tools > Security Manager Administration > Device Communication**, then select **Retrieve while adding devices** in the PIX/ASA/FWSM Device Authentication Certificates field (in SSL Certificate Parameters).

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73
- Commands that Can Cause Conflicts after Rollback , on page 70
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

## Understanding Rollback for IPS and IOS IPS

**Note** From version 4.17, Cisco Security Manager does not support FWSM, IPS, and PIX devices. In addition, from this release, Cisco Security Manager will not provide any enhancements.

Special considerations apply to the rollback of IPS devices and IOS IPS devices. For IPS devices and IOS IPS devices, rollback could possibly include rolling back sensor updates or signature updates. The reason for this is that for IPS devices and IOS IPS devices, Security Manager supports not only the management of configuration but also the support of image management in the form of manual and automatic upgrades and signature updates. Keep in mind that when you do a rollback, you are rolling back the configuration, not the sensor updates or signature updates. These updates are downgraded only if the configuration cannot be rolled back without downgrading the updates.

Rollback is accomplished through Configuration Archive. For IPS devices and IOS IPS devices, only the current configuration is archived. The current configuration for one device version (say, Version X) may not be valid for a different device version (say, Version Y). Security Manager rolls back a configuration of Version X to a sensor with Version Y as long as the configuration for X is valid for Y.

If the configuration for X is valid for Y, rollback proceeds and Security Manager displays a confirmation dialog box to you. If the configuration for X is not valid for Y, Security Manager displays a warning dialog box to you and provides you with the option of downgrading the sensor during rollback if such a downgrade will help accomplish the rollback.

**Caution** Downgrading an IPS device removes certain capabilities of the IPS device. For example, downgrading the engine prevents you from applying the latest signature updates. Operation of an IPS device without the latest signature updates diminishes the effectiveness of the IPS device.

For rollback of a deployment job, the warning dialog box contains one or more of the following types of warnings:

- Security Manager warns you about IPS devices that need to have their sensor version downgraded before a rollback can be performed.
- Security Manager warns you about IOS IPS devices whose signature level has changed. For these devices, only the non-IPS sections of the configuration can be rolled back.
- Security Manager warns you about IPS devices that must be downgraded more than one level, and as a result, Security Manager cannot do it. You must use the Cisco IPS CLI for such downgrades. The warning dialog box displays the version to which the device must be reimaged or downgraded.

**Note** The option of downgrading an IOS IPS device during rollback is not available, because IOS IPS devices do not support downgrade.

If the option of downgrading the sensor during rollback will not help accomplish the rollback, you receive an error message stating that rollback cannot occur and that you need to manually reinstall the image on the device to roll back. Only the update package most recently installed on a device can be downgraded, so downgrade does not help in the following cases:

- Rollback of a deployment (signature update) that involves downloading more than one update package to the device.
- Selection of an old deployment or configuration for rollback subsequent to which several upgrades occurred.
- Rollback of an upgrade that cannot be downgraded. Major, minor, and most service pack upgrades cannot be downgraded, as shown in Table 18: Downgrade Support for Possible Sensor Upgrade Types , on page 69

For rollback of a configuration that requires a downgrade to a version prior to Cisco IPS 5.1(4), Security Manager does not support automatic downgrade. You must manually downgrade the device to the specified version and then proceed with rollback.

***Table 18: Downgrade Support for Possible Sensor Upgrade Types***

| Upgrade Type | Downgrade Support |
|---|---|
| Major Upgrade | Downgrade is not supported. |
| Minor Upgrade | Downgrade is not supported. |
| Service Pack Update | Downgrade from Cisco IPS 5.1(4) onward is not supported. |
| Patch update | Downgrade is supported. |

| Upgrade Type | Downgrade Support |
|---|---|
| Signature Update | Downgrade is supported. |
| Engine Update | Downgrade is supported. |
| Repackage (applicable to major, minor, and service pack updates). | Repackages for service packs prior to 5.1(4) can be downgraded. |

**Caution** Outbreak Prevention updates on a particular device may be lost if that device is downgraded.

During rollback, if Security Manager discovers that there have been out-of-band changes to the device that prevent rollback, you will receive an error message stating that rollback is prevented.

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73

## Commands that Can Cause Conflicts after Rollback

The following commands can potentially cause conflicts after rollback is performed:

- **http server enable** *port***http** *ip_address net_mask interface_name*

Applicable only to security contexts (not the system execution space).

- **allocate-interface** {*physical_interface* | *subinterface* } **[map_name] [visible | invisible]**

Applicable only to the system execution space under the context subcommand.

- **config-url** *diskX:/path/filename*

Applicable only to the system execution space under the context subcommand.

- **join -failover-group** *group_number*

Applicable only for active/active failover and only to the system execution space under the context subcommand. The failover group defaults to group 1 if not specified.

- **failover**

Applicable only to the system execution space. Enabling failover causes configuration synchronization to trigger between peers.

- **failover lan enable**

Applicable only to the system execution space. If this command is omitted, this implies serial cable failover on a PIX platform or warrants an incomplete failover configuration warning on ASA and FWSM.

- **failover lan unit** {*primary* | *secondary* }

Applicable only to the system execution space. If this command is not specified, both units are secondary by default. If rollback takes place on the wrong unit, both can become primary, which impacts which unit becomes active initially.

- **failover group** *group_number*

Applicable only to the system execution space. This command enables active/active failover. If this command is omitted, active/standby is enabled.

- **preempt** *delay*

Applicable only to the system execution space and under the failover group subcommand to force which failover group becomes active if both units are booted up at the same time, or the primary does not boot up within the delay specified.

- **monitor-interface** *interface_name*

Applicable only to security contexts and used to enable health monitoring of critical interfaces. If this interface is 'bounced' or fails, a switchover could occur.

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

## Commands to Recover from Failover Misconfiguration after Rollback

If a switchover happens during rollback and the two units are no longer synchronized, you might need to use the following commands to recover:

- **failover active** *group_number*
- **failover reset** *group_number*
- **failover reload-standby**
- **clear configure failover**

For more information on these commands, please refer to the command reference for your security appliance.

### Related Topics

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72
- Using Rollback to Deploy Archived Configurations , on page 73
- Commands that Can Cause Conflicts after Rollback , on page 70

# Rolling Back Configurations to Devices Using the Deployment Manager

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 cannot roll back to a previous configuration if there are no previous configurations in the Configuration Archive.

You can roll back configurations only to configurations that were deployed to the device, not to a file. For information on how to roll back a configuration that was deployed to a file, see Performing Rollback When Deploying to a File , on page 74.

You can also use the Configuration Archive tool to roll back to any configuration archived from a device. For more information, see Using Rollback to Deploy Archived Configurations , on page 73.

**Caution** Roll back configurations only in extreme circumstances. It is usually a better idea to fix the configuration in Security Manager and deploy the fixed configuration, because rolling back a configuration creates a situation where the configuration defined in Security Manager is not the same one running on the device. After rollback, you should rediscover policies on the device to make the device configuration and its configuration in Security Manager consistent. Roll back configurations only in extreme circumstances. Before proceeding, read the following topics.

- Understanding Configuration Rollback , on page 65
- Understanding Rollback for Devices in Multiple Context Mode , on page 66
- Understanding Rollback for Failover Devices , on page 67
- Understanding Rollback for Catalyst 6500/7600 Devices , on page 67
- Understanding Rollback for IPS and IOS IPS , on page 68
- Commands that Can Cause Conflicts after Rollback , on page 70
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

### Before You Begin

When you roll back a configuration, the action is not done as part of an activity or configuration session, which means the device is not locked. Thus, it is possible that two users might roll back configurations simultaneously on a device, which can generate unexpected problems. Before rolling back a configuration, ensure that there are no active deployment jobs for the device listed in the Deployment Manager window.

### Related Topics

- Viewing Deployment Status and History for Jobs and Schedules , on page 25
- Job States in Non-Workflow Mode , on page 5
- Job States in Workflow Mode , on page 7

**Step 1** Click the **Deployment Manager** button in the Main toolbar. Click the **Deployment Jobs** tab if it is not active.

**Step 2** Select the deployment job (which must be in the Deployed or Failed states) and click **Rollback**.

The Rollback a Job dialog box opens. The dialog box lists all of the devices included in the job, including the name of the device, the deployment method (file or device), the status of the previous deployment, and the name of the deployment job that last updated the device.

**Step 3** Select the devices for which you want to roll back configurations by checking the check box in the Selection column. You can select only devices that used the deploy to device method. By default, all the devices with the status Succeeded are selected.

You can view the configuration that will be deployed to a device by highlighting the row for a device and clicking the **Preview Config** button. You can compare it to the last deployed configuration or the current running configuration. For more information, see Previewing Configurations , on page 44.

**Step 4** Click **OK**. You are asked to confirm the action.

**Step 5** (Optional) To make the configuration defined in Security Manager consistent with the one running on the device, rediscover the device policies as described in Discovering Policies on Devices Already in Security Manager.

# Using Rollback to Deploy Archived Configurations

You can roll back any configuration version from Configuration Archive to the device for which it is archived, provided that the configuration was deployed to the device or originated from the device. The rolled-back configuration then becomes another archived version in the list for that device. For information on how to roll back a configuration that was deployed to a file, see Performing Rollback When Deploying to a File , on page 74.

**Before You Begin**

**Tip** When you roll back a configuration, the action is not done as part of an activity or configuration session, which means the device is not locked. Thus, it is possible that two users might roll back configurations simultaneously on a device, which can generate unexpected problems. Before rolling back a configuration, check the Deployment Manager to ensure that there are no active deployment jobs for the device (select **Manage > Deployments**).

Roll back configurations only in extreme circumstances. Before rolling back configurations, carefully read these topics:

- Understanding Configuration Rollback , on page 65
- Understanding Rollback for Devices in Multiple Context Mode , on page 66
- Understanding Rollback for Failover Devices , on page 67
- Understanding Rollback for Catalyst 6500/7600 Devices , on page 67
- Understanding Rollback for IPS and IOS IPS , on page 68
- Commands that Can Cause Conflicts after Rollback , on page 70
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71

**Related Topics**

- Rolling Back Configurations to Devices Using the Deployment Manager , on page 72

- Adding Configuration Versions from a Device to the Configuration Archive , on page 61
- Managing Deployment, on page 1
- Viewing and Comparing Archived Configuration Versions , on page 61

**Step 1** Select **Manage > Configuration Archive** to open the Configuration Archive (see Configuration Archive Window , on page 23).

**Step 2** In the Device selector, select the device for which you want to roll back to a different configuration version. The archived configurations appear in the right pane.

**Step 3** Select the configuration version to which you want to roll back. You can roll back only to a configuration that was deployed to the device or that originated from the device. You cannot roll back to a configuration that was deployed to a file.

**Tip** To view the configuration version before rollback, click **View**.

**Step 4** Click **Rollback** to deploy the selected configuration version to the device. A progress box appears, followed by a notification message when the configuration version is successfully deployed.

**Step 5** (Optional) To make the configuration defined in Security Manager consistent with the one running on the device, rediscover the device policies as described in Discovering Policies on Devices Already in Security Manager.

However, it is usually better to correct the policies for the device and to then redeploy the updated configuration. This preserves your changes and shared-policy configuration for the device, which would otherwise be removed if you rediscover policies.

# Performing Rollback When Deploying to a File

You cannot directly perform rollback when deploying to a file instead of to a device. Use this procedure to revert to a previously stored configuration when deploying to file.

**Related Topics**

- Understanding Configuration Rollback , on page 65
- Understanding Rollback for Devices in Multiple Context Mode , on page 66
- Understanding Rollback for Failover Devices , on page 67
- Understanding Rollback for Catalyst 6500/7600 Devices , on page 67
- Understanding Rollback for IPS and IOS IPS , on page 68
- Commands to Recover from Failover Misconfiguration after Rollback , on page 71
- Commands that Can Cause Conflicts after Rollback , on page 70

**Step 1** Select **Manage > Configuration Archive** to open the Configuration Archive (see Configuration Archive Window , on page 23).

**Step 2** In the Device selector, select the device for which you want to roll back to a different configuration version. The archived configurations appear in the right pane.

**Step 3** Select the configuration version to which you want to roll back and 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 such as NotePad, then press Ctrl+V to paste the contents of the clipboard into the text file.

**Step 7** Save the file. You can use this file to perform manual rollback.