JUNIPER NETWORKS

Junos® Space

Network Director Deploy Mode User Guide

Release
1.5

Published: 2013-10-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® Space Network Director Deploy Mode User Guide
1.5

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** *metric***>;**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Deploy Mode Overview

Understanding Deploy Mode in Network Director

The Deploy mode enables you to deploy configuration changes and software upgrades to devices and perform several device management and configuration file management tasks.

NOTE: **Deploy mode is disabled for devices in your Virtual view. This is because you can only discover, manage, and monitor devices in your virtual network. None of the deploy mode tasks are applicable to these devices.**

This topic describes:

Deploying Configuration Changes

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode. Every time you make configuration changes in Build mode that affect a device, the device is automatically added to the list of devices with pending changes. Configuration changes are deployed to devices at the device level. When you deploy configuration changes to a device, all pending configuration changes for that device are deployed.

You can do the following configuration deployment tasks on devices that have pending changes:

- Run configuration deployment jobs immediately or schedule them for future times.
- Preview pending configuration changes before deploying.
- Validate that the pending changes are compatible with the device's configuration.
- Manage configuration deployment jobs.

Configuration changes are validated for each device both in Network Director and on the device. If any part of a configuration change for a device fails validation, no configuration changes are deployed to the device. You can see the results of each validation phase separately.

Network Director will not deploy configuration to a device with a configuration that is out of sync (meaning that the device's configuration differs from Network Director's version of that device's configuration), or to a device that has uncommitted changes to its candidate configuration. Deployment to such devices will fail.

When you schedule a deployment job, that job and any profiles and devices assigned to that job are locked within Network Director. You cannot edit the job or any of its assigned profiles until the job runs or gets cancelled. This locking feature prevents you from deploying unintended configuration changes that could result from editing profiles and devices that are already scheduled to deploy. To change any properties of a scheduled job, cancel the job and create a new scheduled job with the desired properties. You cannot edit the profile assignments of a device that has scheduled pending configuration changes.

Managing Software Images

Network Director can manage software images on the nodes it manages. You can do the following software image management tasks:

- Deploy a software image stored in an image repository on the Network Director server to multiple devices with a single job.
- Track the status of software image management jobs.
- Stage and install software images as separate tasks.
- Schedule staging and installation to happen at independent future times.
- Perform several software image upgrade options, such as rebooting devices automatically after the upgrade finishes.

NOTE: **Using nonstop software upgrade (NSSU) to upgrade EX Series switches is supported in Network Director release 1.5.**

Zero Touch Provisioning

Zero touch provisioning enables you to provision new Juniper Networks switches in your network automatically—without manual intervention. When you physically connect a

switch to a network and boot it with the factory-default configuration, the switch attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network.

Managing Devices

In Deploy mode you can perform several device management tasks, including:

- View the device inventory.
- Show a device's current configuration.
- Resynchronize the device configuration maintained in Build mode with the configuration on the device. For more information about resynchronization of device configuration, see "Understanding Resynchronization of Device Configuration" on page 10
- Convert access points that were added to a controller using an Auto AP profile configuration to a persistent access point configuration on the controller.
- Enable or disable switch network ports.
- Manage QFabric node groups.
- Convert QSFP+ port configuation.

Managing Device Configuration Files

You can back up device configuration files to the Network Director server. You can perform several actions on backed up configuration files, such as restoring configuration files to devices, and viewing and comparing configuration files.

Related Documentation

- Deploying Configuration to Devices on page 19
- Deploying Software Images on page 35
- *Viewing the Device Inventory Page*
- Viewing a Device's Current Configuration from Network Director on page 61
- Resynchronizing Device Configuration on page 56
- Enabling or Disabling Network Ports on Switches on page 56
- Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director on page 49
- Managing Device Configuration Files on page 63

Understanding the Deploy Mode Tasks Pane

The Tasks pane in Deploy mode lists the available tasks. All Deploy mode tasks are always available, regardless of the scope selected in the View pane.

Deploy mode tasks are divided into the following categories:

- **Configuration Deployment**—These tasks enable you to deploy configuration changes to devices and manage configuration deployment jobs. Table 3 on page 6 describes the configuration deployment tasks.
- **Image Management**—These tasks enable you to manage software images on devices. Table 4 on page 6 describes the image management tasks.
- **Device Management**—These tasks enable you to view the device inventory, resynchronize the configuration of out-of-sync devices, manage the administrative state of ports, manage QFabric node groups, and convert QSFP+ port configuration. Table 5 on page 7 describes the device management tasks.
- **Device Configuration File Management**—These tasks enable you manage configuration files on managed devices. Table 6 on page 7 describes the device configuration file management tasks.
- **Zero Touch Provisioning**—These tasks enable you to provision new Juniper Networks switches in your network automatically—without manual intervention. Table 7 on page 7 describes the zero touch provisioning tasks.
- **Key Tasks**—Network Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Network Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

Table 3 on page 6 through Table 6 on page 7 describe the tasks in each task category.

Table 3: Configuration Deployment Tasks

Task	Description
Deploy Configuration Changes	Deploys pending configuration changes to devices.
Set SNMP Trap Configuration	Enables SNMP traps on network devices so that Network Director can collect and manage event and error information from these devices.
View Deployment Jobs	Manages configuration deployment jobs.

Table 4: Image Management Tasks

Task	Description
Manage Image Repository	Manages the software images repository on the server.

Table 4: Image Management Tasks *(continued)*

Task	Description
Deploy Images to Devices	Deploys software images from the repository to devices.
View Image Deployment Jobs	Manages software image deployment jobs.

Table 5: Device Management Tasks

Task	Description
Convert Auto AP	Converts access points that were added to a controller using an Auto AP profile configuration to a persistent access point configuration on the controller.
Convert Ports	Converts QSFP+ port configuration.
Manage Node Groups	Manages QFabric node groups.
Manage Port Admin State	Enables or disables switch network ports.
Resynchronize Device Configuration	Resynchronizes the device configuration maintained in Build mode with the running configuration on the devices.
Show Current Configuration	Shows the selected device's current configuration.
View Inventory	Displays the device inventory of the selected node.

Table 6: Device Configuration File Management Tasks

Task	Description
Manage Device Configuration Files	Manages backup device configuration files.
View Configuration File Mgmt Jobs	Manages device configuration file management jobs.

Table 7: Zero Touch Provisioning Tasks

Task	Description
Setup	Set up the zero touch provisioning profile to configure the DHCP server and to upload the software image and configuration file to a file server.
Monitor	View details of the devices that are provisioned using a given zero touch provisioning profile.

Related Documentation

- Understanding Deploy Mode in Network Director on page 3
- *Understanding the Network Director User Interface*

Understanding Node Groups

Node groups help you combine multiple QFabric Node devices into a single virtual entity within the QFabric system to enable redundancy and scalability at the edge of the data center.

This topic covers:

Network Node Groups

A set of one or more Node devices that connect to an external network is called a *network Node group*. The network Node group also relies on two external Routing Engines running on the Director group. These redundant *network Node group Routing Engines* run the routing protocols required to support the connections from the network Node group to external networks.

When configured, the Node devices within a network Node group and the network Node group Routing Engines work together in tandem as a single entity. By default, network Node group Routing Engines are part of the **NW-NG-0** network Node group but no Node devices are included in the group. As a result, you must configure Node devices to be part of a network Node group.

In a QFabric system deployment that requires connectivity to external networks, you can modify the automatically generated network Node group by including its preset name **NW-NG-0** in the Node group configuration. Within a network Node group, you can include a minimum of one Node device up to a maximum of eight Node devices. By adding more Node devices to the group, you provide enhanced scalability and redundancy for your network Node group.

NOTE: The QFabric system creates a single **NW-NG-0** network Node group for the default partition. You cannot configure a second network Node group inside the default partition. The remaining Node devices within the default partition are reserved to connect to servers, storage, or other endpoints internal to the QFabric system. These Node devices either can be retained in the automatically generated server Node groups or can be configured as part of a redundant server Node group.

Server Node Groups

A *server Node group* is a set of one or more Node devices that connect to servers or storage devices. Unlike Node devices that are part of a network Node group and rely on an external Routing Engine, a Node device within a server Node group connects directly to endpoints and implements the Routing Engine functions locally, using the local CPU built into the Node device itself.

By default, each Node device is placed in its own self-named autogenerated server Node group to connect to servers and storage. You can override the default assignment by manually configuring a redundant server Node group that contains a maximum of two Node devices. You can use a redundant server Node group to provide multihoming services to servers and storage, as well as configure aggregated LAG connections that span the two Node devices.

NOTE: The Node devices in a redundant server Node group must be of the same type, either a QFX3500 Node device or a QFX3600 Node device. You cannot add a QFX3500 and a QFX3600 Node device to the same redundant server Node group.

Related Documentation

- Creating and Managing Node Groups on page 53
- *Setting Up QFabrics*

Understanding Resynchronization of Device Configuration

In a network managed by Network Director, three separate repositories about device configuration are maintained:

- The configuration information on the devices themselves. Each switch and wireless LAN controller maintains its own configuration record.
- The configuration information maintained by the Junos Space Network Management Platform. When a device is discovered, either by Junos Space or Network Director, Junos Space stores a record of the configuration on that device.

  Network Director uses the configuration record maintained by Junos Space to determine what configuration commands need to be sent to the device when you deploy configuration on the device in Deploy mode.
- The configuration information maintained by Network Director in Build mode. This information takes the form of the profiles assigned to the device, plus the additional configuration, such as LAG and access point configuration, that you can do under device management.

In Network Director, the configuration state of a device is shown as In Sync when the configuration information in all three repositories match. If there is a conflict between the configuration information in one or more of the repositories, Network Director shows the device configuration state as Out of Sync.

An Out of Sync state is usually the result of out-of-band configuration changes—that is, configuration changes made to a device using a management tool other than Network Director. Examples of such changes include changes made by:

- Using the device CLI.
- Using the device Web-based management interface (the J-Web interface or Web View).
- Using the Junos Space Network Management Platform configuration editor.

NOTE: **You cannot use the Junos Space configuration editor to configure wireless LAN controllers.**

- Using RingMaster software.
- Restoring or replacing device configuration files.

You cannot deploy configuration on a device when the device configuration state is Out of Sync.

This topic describes how Network Director enables you to resynchronize the device configuration state. It covers:

- The Resynchronize Device Configuration Task on page 11

The Resynchronize Device Configuration Task

Network Director provides a task in Deploy mode that enables you to resynchronize the repositories of configuration information. When an out-of-band configuration change is made, you can use this task to resynchronize both the Junos Space configuration record and the Build mode configuration with the configuration on the device.

How Network Director performs resynchronization depends on the system of record (SOR) mode set for the Junos Space Network Management Platform. There are two possible modes:

- Network as system of record (NSOR). This is the default mode.
- Junos Space as system of record (SSOR).

You set the mode in Junos Space under Administration > Applications > Network Management Platform > Modify Application Settings.

How Resynchronization Works in NSOR Mode

In NSOR mode, the network device is considered the system of record for device configuration, which means the configuration maintained by the device takes precedence over the configuration maintained by Junos Space and Network Director. Thus when you perform a resynchronization, the Junos Space configuration record and the Network Director Build mode configuration are updated to match the device configuration.

When an out-of-band change is made on a managed device when Junos Space is in NSOR mode:

1. Junos Space detects that a configuration change has occurred on the device and informs Network Director about the change.
2. Both Junos Space and Network Director set the device configuration state to Out of Sync.
3. Junos Space automatically resynchronizes its configuration record to match the device configuration and sets the device configuration state to In Sync when the synchronization completes.
4. If the configuration change does not affect configuration that you can perform in Build mode (for example, routing configuration), Network Director also sets the device configuration state to In Sync after the Junos Space resynchronization completes. All three configuration repositories are now in sync.

   If the configuration change affects configuration that you can perform in Build mode, Network Director does not set the device configuration state to In Sync. Instead, it continues to show the device configuration state as Out of Sync because the Build mode configuration does not match the device configuration.

5. To resolve the Out of Sync state in Network Director, use the Resynchronize Device Configuration task in Deploy mode. Network Director updates the Build mode configuration to match the out-of-band changes.
6. Network Director sets the device configuration state to In Sync.

NOTE: Automatic resynchronization, as described in Step 3 above, is a default setting for the Junos Space Network Management Platform. If automatic resynchronization is disabled, you must manually resynchronize the Junos Space configuration with the device configuration. You can do so in two ways:

- Use the Resynchronize with Network action in Junos Space. The Junos Space configuration is synchronized with the device configuration. However, the Build mode configuration is not synchronized, so the device state in Network Director remains Out of Sync. You must use the Resynchronize Device Configuration task in Deploy mode to resynchronize the Build mode configuration.
- Use the Resynchronize Device Configuration task in Deploy mode. In this case, Network Director resynchronizes both the Junos Space configuration and the Build mode configuration with the device configuration.

How Resynchronization Works in SSOR Mode

When Junos Space is in SSOR mode, Junos Space is considered the system of record for device configuration. In this mode, when an out-of-band configuration change occurs on a device, you can choose whether to accept the change or to overwrite the change with the configuration maintained by Junos Space.

When an out-of-band change is made on a managed device when Junos Space is in SSOR mode:

1. Junos Space detects that a configuration change has occurred on the device and informs Network Director about the change.
2. Junos Space sets the device configuration state as Device Changed, and Network Director sets the device configuration state to Out of Sync.

   Network Director sets the device configuration state to Out of Sync even if the configuration change does not affect configuration you can perform in Build mode. This allows you to resolve the Device Changed configuration state for Junos Space from Network Director.
3. In Network Director, use the Resynchronize Device Configuration task to accept or reject the out-of-band changes:
   - If you accept the out-of-band changes, both the Junos Space configuration record and the Network Director Build mode configuration are resynchronized to reflect the out-of-band configuration changes.

- If you reject the out-of-band changes, the configuration on the device is overwritten by the configuration record maintained by Junos Space. The Network Director Build mode configuration remains unchanged.

4. Both Junos Space and Network Director set the device configuration state to In Sync.

The above process differs somewhat when out-of-band configuration changes are made through the Junos Space configuration editor. In this case:

1. Junos Space sets the device configuration state as Space Changed after the configuration change is saved.

   At this point, the changes have been made only in the Junos Space configuration record and the changes have not yet been deployed to the device. Network Director shows the device configuration state as In Sync.

   

   NOTE: **Because the device configuration state is In Sync in Network Director, you can deploy configuration on the device from Network Director at this point. If you do so, the Network Director changes are deployed on the device, but the Junos Space changes are not. The device state in Junos Space remains Space Changed.**

2. When the changes are deployed to the device from Junos Space, Junos Space changes the device state to In Sync, while Network Director changes the device state to Out of Sync.
3. In Network Director, use the Resynchronize Device Configuration task to resolve the Out of Sync state. In this case, because the Junos Space configuration record and the device configuration are in sync, you cannot reject the changes. When you resynchronize the device in Network Director, the Build mode configuration is updated to reflect the configuration changes.
4. Network Director sets the device configuration state to In Sync.

If you use Junos Space instead of Network Director to resolve out-of-band configuration changes in SSOR mode, note the following:

- If you reject an out-of-band change, the device state becomes In Sync in both Network Director and Junos Space.
- If you accept an out-of-band change that does not affect the Build mode configuration, the device state becomes In Sync in both Network Director and Junos Space.
- If you accept an out-of-band change that affects the Build mode configuration, the device state becomes In Sync in Junos Space but remains Out Of Sync in Network Director. You must use the Resynchronize Device Configuration task to resolve the Out of Sync state.

NOTE: When Junos Space is in SSOR mode, we recommend that you do not make out-of-band changes to the cluster configuration on the secondary seeds and member controllers of a mobility domain, such as disabling the cluster on these devices. Use Network Director to modify the cluster configuration on these devices.

How Network Director Resynchronizes the Build Mode Configuration

When you use the Resynchronize Device Configuration task to resynchronize the Build mode configuration to the device configuration, Network Director launches a resynchronization job. This job deletes all profile assignments configured for the device. The profiles themselves are not deleted—just the assignments of the profiles to the device are deleted. It then reimports the device configuration, as if the device were a newly discovered device. It reassigns existing profiles and creates new profiles as necessary. Profiles that were originally assigned to the device will be reassigned to the device if the profiles were unaffected by the out-of-band changes. All profiles assigned to the device are in a deployed state at the end of the process. Any profile that is not reassigned to the device and is not assigned to any other device will be in a unassigned state.

Related Documentation

- Resynchronizing Device Configuration on page 56

Understanding Zero Touch Provisioning in Network Director

Zero touch provisioning allows you to provision new Juniper Networks switches in your network automatically—without manual intervention. When you physically connect a switch to a network and boot it with the factory-default configuration, the switch attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network. Use the Zero Touch Provisioning wizard to create a profile that applies all the configurations to a Dynamic Host Configuration Protocol (DHCP) server that you configure. You can apply one or more profiles to a DHCP server.

After you enable zero touch provisioning for a DHCP server that is part of a given subnet in your network, and connect a new switch to that subnet, the following series of events occurs:

1. The switch contacts the DHCP server to obtain an IP address. The DHCP server assigns an IP address to the switch. The DHCP server also passes on the location of the software image, and the configuration file to the switch. This information is passed on to the DHCP server from Network Director when you create and save a zero touch provisioning profile.
2. The switch uses this information to locate the software image, and the configuration file. These files are stored in an FTP, TFTP, or an HTTP server.
3. The switch then upgrades the operating system version by using the software image and loads the configuration file.

NOTE: You can use zero touch provisioning to provision EX Series switches to run Junos OS Release 12.3R5 and 13.3 only. If a switch is provisioned with any other Junos OS Release, then Step 4 is not applicable. You must manually discover the switch from Network Director to be able to manage it.

4. After a successful upgrade, the switch sends out an trap message to Network Director to announce that a new switch has been deployed in the network. If the trap message is successfully received, Network Director adds the switch to the Network Director's inventory. This eliminates the need to manually discover new devices that are added to your switching network.

NOTE: if the SNMP trap that the switch sends to Network Director does not reach the destination, then Network Director does not know about the new device and the device will not be added to the Network Director's inventory. In such a scenario, you must manually discover the new device from Network Director.

For more information on zero touch provisioning for switches, see Understanding Zero Touch Provisioning.

Related Documentation

- Configuring and Monitoring Zero Touch Provisioning on page 43

PART 2

Administration

CHAPTER 2

Configuration Management

Deploying Configuration to Devices

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode.

To start deploying configuration changes:

1. Click **Deploy** in the Network Director banner.
2. Select a node in the View pane that contains the devices to which you want to deploy.
3. In the Tasks pane, select **Configuration Deployment > Deploy Configuration Changes**.

   The Devices with Pending Changes page opens in the main window, listing the devices within the selected node that have pending configuration changes.

This topic describes:

Selecting Configuration Deployment Options

From the Devices with Pending Changes page, you can:

- Deploy configuration changes immediately by selecting one or more devices and clicking Deploy Now. For more information, see "Deploying Configuration Changes to Devices Immediately" on page 21.
- Schedule configuration deployment by selecting one or more devices and clicking Schedule Deploy. For more information, see "Scheduling Configuration Deployment" on page 21.
- View configuration changes that are pending on a device by selecting the device and clicking View Pending Configuration Changes. For more information, see "Viewing Pending Configuration Changes" on page 22.
- Validate that the pending changes for a device are compatible with the device's configuration by selecting up to ten devices and clicking Validate Pending Configuration Changes. For more information, see "Validating Configuration" on page 22.

NOTE: **You cannot delete a device from the Devices with Pending Changes list. To remove a device from the list, you must undo the Build mode configuration changes that placed the device on the list.**

Table 8 on page 20 describes the information provided in the table on the Devices with Pending Changes page. Only the subset of devices within the selected object that have pending configuration changes are listed in the table.

Table 8: Devices with Pending Changes Page

Table Column	Description
Check box	Select to perform an action on the device in that row
Name	Device name
IP Address	Device IP address
Model	Device Model
OS Version	Operating system version running on device
Connection State	State of the connection to the device: • Up—Network Director can communicate with the device. • Down—Network Director cannot communicate with the device. You cannot deploy configuration to devices that are down.

Table 8: Devices with Pending Changes Page *(continued)*

Table Column	Description
Configuration State	Indicates whether the device's configuration is in sync with Network Director's version: • In Sync—The configuration on the device is in sync with the Network Director configuration for the device. • Out Of Sync—The configuration on the device does not match the Network Director configuration for the device. This state is usually the result of the device configuration being altered outside of Network Director. You cannot deploy configuration on a device when the device is Out Of Sync. To resolve this state, use the Resynchronize Device Configuration task in Deploy mode. • Synchronizing—The device configuration is in the process of being resynchronized. • Sync failed—An attempt to resynchronize an Out Of Sync device failed.

Deploying Configuration Changes to Devices Immediately

To deploy configuration changes to devices immediately:

1. Select the device or devices in the Devices with Pending Changes page.
2. Click **Deploy Now**.

   The Deploy Options window opens.
3. In the Deploy Options window, enter a job name in the Deployment Job Name field, then click **OK**.

   The configuration deployment job runs. The Deploy Configuration window opens and shows the results of the deployment job. See for a description of this window, see "Deploy Configuration Window" on page 26.

Scheduling Configuration Deployment

To schedule configuration deployment to devices:

1. Select the device or devices in the Devices with Pending Changes page.
2. Click **Schedule Deploy**.

   The Deploy Options window opens.
3. Use the Deploy Options window to schedule the configuration deployment. See "Specifying Configuration Deployment Scheduling Options" on page 21 for a description of the window.

Specifying Configuration Deployment Scheduling Options

Use the Deploy Options window to schedule configuration deployment jobs. Table 9 on page 22 describes the actions for the fields in this window.

Table 9: Deploy Options Window

Field	Action
Deployment Job Name	Enter a job name.
Date and Time	Enter the job's start date and time.
OK	Click to accept changes and exit the window.
Cancel	Click to cancel changes and exit the window.

Viewing Pending Configuration Changes

To view pending configuration changes on devices:

1. Select the device or devices in the Devices with Pending Changes page.
2. Click **View Pending Configuration Changes**.

   The Pending Changes window opens. See "Using the Pending Changes Window" on page 22 for a description of the window.

Validating Configuration

When you deploy configuration changes to a device, validation checks are performed to validate that the pending changes are compatible with the device. You can also perform this validation without deploying.

NOTE: **You can also verify the configuration from the Build mode by clicking Tasks > Domain Management > Validate Pending Configuration.**

To validate that the pending changes for devices are compatible with the device configuration:

1. Select up to ten devices in the Devices with Pending Changes page.
2. Click **Validate Pending Configuration Changes**.

   The Configuration Validation window opens. See "Using the Configuration Validation Window" on page 24 for a description of the window.

Using the Pending Changes Window

Use the Pending Changes window to view the pending Network Director changes for a device. Table 10 on page 23 describes the fields in this window.

Table 10: Pending Changes Window

Field	Description
Name	Lists each selected device. Expand a device by clicking on its plus sign to see its pending changes. Each pending change to a profile or other configuration object for the device is listed.
State	Describes the nature of the pending change to the configuration object. These are the possible states: • Added—The profile or configuration object was added to this device. • Removed—The profile or configuration object was removed from the device • Updated—The profile or configuration object was updated.
Configuration	Click **View** to view the pending configuration changes for a device. The Pending Configuration window opens. See "Using the Configuration or Pending Configuration Window" on page 23 for information about the window. NOTE: The device configuration state must be In Sync for you to view the pending configuration changes.
Close	Click to close the window.

Using the Configuration or Pending Configuration Window

Use the Pending Configuration window to view the configuration changes that will be deployed to a device when a job runs. Use the Configuration window to see changes that were deployed to a device when a completed job ran. The configuration changes are shown in these formats:

- Select the **XML View** tab to view the configuration changes in XML format. This view shows the XML-formatted configuration that will be deployed to the device's Device Management Interface (DMI), which is used to remotely manage devices.
- Select the **CLI View** tab to view the configuration changes in CLI format. This view shows the Junos configuration statements that will be deployed to the device.

In both views, the content is color-coded for easier reading:

- Black text indicates configuration that is already active on the device, and will not be changed if you deploy.
- Green text indicates configuration that will be added if you deploy.
- Red text indicates configuration that will be removed if you deploy.

Using the Deploy Configuration Errors/Warnings Window

Use the Deploy Configuration Errors/Warnings window to view the results of deploying configuration to a device. The Errors/Warnings in validating the device configuration pane shows the results of configuration validation by Network Director. The Errors/Warnings in Updating Device configuration pane shows the results of configuration validation on the device.

Using the Configuration Validation Window

Use the Configuration Validation window to validate that the pending changes for a device are compatible with the device's configuration. Table 11 on page 24 describes this window.

Table 11: Configuration Validation Window

Table Column	Description
Object name	Lists the devices you selected for validation. Click the arrow next to a device to expand it. If there are no errors or warnings, one item labeled No Validation warnings appears. If the device has errors or warnings, they appear under the device. The device contains a list of the profiles that caused errors or warnings. Expand a profile name to see the of errors and warnings it caused.
Errors/Warnings	Describes the error or warning.

Related Documentation

- Deploying Configuration Changes on page 3
- Managing Configuration Deployment Jobs on page 24

Managing Configuration Deployment Jobs

When you deploy configuration changes or schedule a configuration deployment, a configuration deployment job is created.

To start managing configuration deployment jobs:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Device Management > View Deployment Jobs**.

   The Deploy Configuration page opens in the main window. The table on that page lists configuration deployment jobs.

This topic describes:

- Selecting Configuration Deployment Job Options on page 24
- Viewing Configuration Deployment Job Details on page 25
- Canceling Configuration Deployment Jobs on page 25

Selecting Configuration Deployment Job Options

From the Deploy Configuration page, you can:

- View the details of a configuration deployment job by clicking Show Details. See "Viewing Configuration Deployment Job Details" on page 25 for more information.
- Cancel a scheduled configuration deployment job by clicking Cancel Job. See "Canceling Configuration Deployment Jobs" on page 25 for more information.

Table 12 on page 25 describes the information provided on the Deploy Configuration page

Table 12: Deploy Configuration Table Description

Table Column	Description
Check box	Select to perform an action on the job in that row.
Job Id	An identifier assigned to the job.
Job Name	Job name (user-created).
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is applied if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is applied if all of the devices in the job completed successfully.
Summary	Job summary.
Scheduled Start Time	Job's scheduled start time
Actual Start Time	Time when the job started.
End Time	Time when the job ended
User	User who created the job
Recurrence	This field is not used for configuration deployment jobs.

Viewing Configuration Deployment Job Details

To view the details of a configuration deployment job:

1. Select the job in the table.
2. Click **Show Details**. The Deploy Configuration window opens. See "Deploy Configuration Window" on page 26 for a description of the window.

Canceling Configuration Deployment Jobs

To cancel a configuration deployment job:

1. Select the job in the table.
2. Click **Cancel Job**.

3. Click **Yes** in the confirmation window that opens.

Related Documentation

- Deploying Configuration Changes on page 3
- Deploying Configuration to Devices on page 19

Deploy Configuration Window

The Deploy Configuration window shows the results of a completed deployment job or information about a scheduled job. See Table 13 on page 26 for a description of the fields in this window.

Table 13: Deploy Configuration Window

Field	Description
Job Name	Job name.
Job Start Time	Time when job started or will start.
Job End Time	Time when job ended.
Percentage Completed	Percentage of the job that is complete.
Number of Devices	Number of devices in the deployment job.
Deployed Devices table	
Name	Device name.
IP Address	Device IP address.
Deployment Status	Status of configuration deployment on device: • Scheduled—Job is scheduled for future deployment. • In Progress—Deployment is in progress. • Success—Deployment completed successfully. • Failed—Deployment failed.
Configuration	Click **View** to see the configuration changes that were deployed to the device. See "Using the Configuration or Pending Configuration Window" on page 23 for more information. For a scheduled job, this column does not contain a link. See "Deploying Configuration to Devices" on page 19 for information about viewing pending configuration changes for a device.
Result Details	Click **View** to see the results of configuration deployment for the device. See "Using the Deploy Configuration Errors/Warnings Window" on page 23 for more information.
Close	Click to close the window.

Related Documentation

- Deploying Configuration Changes on page 3
- Deploying Configuration to Devices on page 19
- Managing Configuration Deployment Jobs on page 24

Enabling SNMP Categories and Setting Trap Destinations

SNMP traps must be enabled on network devices for Network Director to collect and manage event and error information from these devices.

Network Director organizes switch and controller traps by categories. These categories must be enabled and deployed in order to forward trap information to Network Director.

NOTE: **Network Director uses protocol port 10162 for receiving traps from devices. This port must be open on the devices.**

This topic describes:

- Viewing Eligible Devices for Trap Forwarding on page 27
- Enabling Trap Forwarding on page 28
- Deploying SNMP Trap Configurations on page 28

Viewing Eligible Devices for Trap Forwarding

Traps are enabled on the Devices page in Deploy mode. To locate this page:

1. Select **Deploy** in the Network Director banner.
2. Select **Set SNMP Trap Configuration** in the Tasks pane. The Devices page opens. For a description of fields in the Devices page, view Table 14 on page 27.

Table 14: Device Page Fields

Field	Description
Name	Either the hostname or the IP address of the device.
IP Address	Device IP address.
Model	Device model number.
OS Version	Version and release level of the operating system running on the device.
Connection State	State of connection to the device. Valid states are: • Up—Network Director is in communication with the device. • Down—Network Director cannot communicate with the device. You cannot enable traps on devices that are in this state.

Table 14: Device Page Fields *(continued)*

Field	Description
Configuration State	Either the device's configuration is in sync or out-of-sync with Network Director's version: • IN_SYNC—The configuration is in-sync with the database. • OUT_OF_SYNC—The configuration is out-of-sync with the database.

Enabling Trap Forwarding

Select **Set SNMP Trap Configuration** in Deploy mode to enable your network devices to pass SNMP traps and events to Network Director. Network Director creates a target group called *networkdirector_trap_group* using target port 10162. The Community name is *public* and the access is *read-write-notify.*.

Before enabling trap forwarding, complete device discovery for all the devices and ensure they are in the up state. Down devices cannot be enabled for trap forwarding.

Selecting Set SNMP Trap Configuration displays the Devices page which contains a table of all discovered switches and controllers in the network. To enable SNMP traps on switches and controllers:

1. Either select individual check boxes for devices, or select the check box next to the Name heading to select all devices. These devices must be up and in the same device family. So if you have both wireless devices and switches, you need to deploy the trap configurations in separate passes.
2. Click **Deploy Trap Configuration**. The Deploy Options window opens.
3. Fill in a new deployment job name or accept the default name of Deploy SNMP Targets.
4. Either select check boxes for individual traps, or select the check box next to the Trap Name heading to select all traps. These traps are discussed further in "Deploying SNMP Trap Configurations" on page 28.

   TIP: **To clear an existing configuration, do not select any of the check boxes.**

5. Click **Ok**. The Deploy Configuration window opens, which shows the status of deploying the configuration change.
6. Review the outcome of the deployment.

After enabling the traps, enable the alarms and establish the alarm retention period. These tasks are located in Preferences in the Network Director banner.

Deploying SNMP Trap Configurations

The Deploy Options for trap forwarding enable you to select individual traps or all traps for the selected device family.

The device family determines which traps are displayed in the Deploy Options window. The following tables map the trap to one or more MIBs being used.

- EX Series switches traps and related MIBs are shown in Table 15 on page 29.
- Controllers traps and related MIBs are shown in Table 16 on page 29.

Table 15: EX Series Switches Traps

Trap	MIB
Chassis	jnxExMibRoot.mib
Link	snmpTraps.mib
Configuration	jnxCfgMgnt.mib
Authentication	jnxJsAuth.mib
Remote operations	jnxPing.mib
Routing	jnx-ipv6.mib
Startup	snmpTraps.mib
Rmon-alarm	jnxRmon.mib
Vrrp-events	rfc2787a.mib
Services	jnxServices.mib
Sonet-alarms	jnx-sonetaps.mib
Otn-alarms	jnxMIbs.mib

Table 16: Controllers Traps

Trap	MIB
LinkDown	snmpTraps.mib
LlinkUp	snmpTraps.mib
Authentication	snmpTraps.mib
DeviceFail	trpzTrapsV2.mib
DeviceOkay	trpzTrapsV2.mib
PoEFail	trpzTrapsV2.mib
MobilityDomainJoin	trpzTrapsV2.mib

Table 16: Controllers Traps *(continued)*

Trap	MIB
MobilityDomainTimeout	trpzTrapsV2.mib
RFDetectAdhocUser	trpzTrapsV2.mib
ClientAuthenticationFailure	trpzTrapsV2.mib
ClientAuthorizationFailure	trpzTrapsV2.mib
ClientAssociationFailure	trpzTrapsV2.mib
ClientDeAssociation	trpzTrapsV2.mib
ClientRoaming	trpzTrapsV2.mib
AutoTuneRadioPowerChange	trpzTrapsV2.mib
AutoTuneRadioChannelChange	trpzTrapsV2.mib
CounterMeasureStart	trpzTrapsV2.mib
CounterMeasureStop	trpzTrapsV2.mib
ClientDot1xFailure	trpzTrapsV2.mib
RFDetectDoS	trpzTrapsV2.mib
RFDetectDoSPort	trpzTrapsV2.mib
ClientIpAddrChange	trpzTrapsV2.mib
ClientAssociationSuccess	trpzTrapsV2.mib
ClientAuthenticationSuccess	trpzTrapsV2.mib
ClientDeAuthentication	trpzTrapsV2.mib
RFDetectBlacklisted	trpzTrapsV2.mib
RFDetectAdhocUserDisappear	trpzTrapsV2.mib
ApRejectLicenseExceeded	trpzTrapsV2.mib
ClientDynAuthorChangeSuccess	trpzTrapsV2.mib
ClientDynAuthorChangeFailure	trpzTrapsV2.mib
ClientDisconnect	trpzTrapsV2.mib

Table 16: Controllers Traps *(continued)*

Trap	MIB
MobilityDomainFailOver	trpzTrapsV2.mib
MobilityDomainFailBack	trpzTrapsV2.mib
RFDetectRogueDeviceDisappear	trpzTrapsV2.mib
RFDetectSuspectDeviceDisappear	trpzTrapsV2.mib
RFDetectedClientViaRogueWiredAP	trpzTrapsV2.mib
RFDetectedClassificationChange	trpzTrapsV2.mib
ConfigurationSaved	trpzTrapsV2.mib
APNonOperStatus	trpzTrapsV2.mib
MichaelMICFailure	trpzTrapsV2.mib
ApManagerChange	trpzTrapsV2.mib
ClientCleared	trpzTrapsV2.mib
MobilityDomainResiliencyStatus	trpzTrapsV2.mib
ApOperRadioStatus	trpzTrapsV2.mib
ClientAuthorizationSuccess	trpzTrapsV2.mib
RFDetectRogueDevice	trpzTrapsV2.mib
RFDetectSuspectDevice	trpzTrapsV2.mib
ClusterFailure	trpzTrapsV2.mib
MultimediaCallFailure	trpzTrapsV2.mib
ApTunnelLimitExceeded	trpzTrapsV2.mib
WsTunnelLimitExceeded	trpzTrapsV2.mib
RFNoiseSource	trpzTrapsV2.mib
M2UConvNotPossibleTrap	trpzTrapsV2.mib
M2UConvAvailablityRestored	trpzTrapsV2.mib

Related Documentation

- *Setting Up User and System Preferences*
- *Understanding Fault Mode in Network Director*

CHAPTER 3

Software Image Management

Managing Software Images

This topic describes how to manage software images for managed devices.

To start managing software images:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Image Management > Manage Image Repository**.

   The Device Image Repository page opens in the main window. The table lists the software images in the repository.
3. In the Tasks pane, select **Device Configuration File Management > Manage Device Configuration**.

   The Manage Device Configuration page opens in the main window. The table lists the devices that have configuration files backed up software images in the repository.

This topic describes:

Selecting Software Image Management Options

From the Device Image Repository page, you can:

- Add a software image to the repository by clicking Add.
- View details about a software image by selecting it and clicking Details.

- Delete software images from the repository by selecting them and clicking Delete.

Table 17 on page 34 describes the information provided in the Device Image Repository table.

Table 17: Device Image Repository Table

Table Column	Description
Check box	Select to perform an action on the software image in that row.
Name	Software image name.
Version	Software version.
Series	Device series that uses the software image.
Uploaded By	User who uploaded the software image.
Created On	Time when the software image was uploaded to the server.
Size(MB)	Size of the software image in megabytes.

Adding Software Images to the Repository

Software images are stored in a repository on the Network Director server.

To add a software image to the repository:

1. Click **Add**.

   The Device Image Upload window opens.

2. Use the Device Image Upload window to upload a device software image. See "Using the Device Image Upload Window" on page 34 for a description of the window.

Using the Device Image Upload Window

To use the Device Image Upload window to add a software image to the repository:

1. Click **Browse** and browse to the software image file.
2. Click **Upload** to add the file to the repository.

Viewing Software Image Details

To view details about a software image:

1. Select the software image file in the table.
2. Click **Details**.

   The Device Image Summary window opens. See "Using the Device Image Summary Window" on page 35 for information about this window.

Using the Device Image Summary Window

Use the Device Image Summary window to view detailed information about a software image. Table 18 on page 35 describes the fields in this window.

Table 18: Device Image Summary Window

Field	Description
Name	Software image filename.
Version	Software version (release number).
Series	Device series on which the software is supported.
Supported Platforms	Platforms on which the software is supported.
Uploaded By	User who uploaded the image to the server.
Created On	Date and time when the software image was uploaded.
Size (MB)	Size of the software image file, in megabytes.
OK	Click to close the window.

Deleting Software Images

To delete software image files:

1. Select the check box in the rows of the software image files that you want to delete.
2. Click **Delete**.

Related Documentation

- Managing Software Images on page 4
- Deploying Software Images on page 35
- Managing Software Image Deployment Jobs on page 39

Deploying Software Images

This topic describes how to deploy software images to managed devices. You must upload software images to the Network Director server before you can deploy them to devices. See "Managing Software Images" on page 33 for more information.

To start deploying software images:

1. Click **Deploy** in the Network Director banner.
2. Select a node in the View pane that contains the devices to which you want to deploy software images.

3. In the Tasks pane, select **Image Management > Deploy Images to Devices**.

   The Select Devices page of the Deploy Images to Devices wizard opens in the main window.

This topic describes:

Specifying Software Deployment Job Options

To specify software deployment job options in the Select Devices page:

1. In the Job name field, enter a job name.
2. From the Device and deployment options list, select an option:
   - Select **Staging only (Download image to the device)** to download the software image to the device but not install it.
   - Select **Upgrade only (Install previously staged image on device)** to upgrade the device to a software image that was previously staged on the device.
   - Select **Staging and Upgrade (Download and Install image on device)** to download the software image and install it on the device.

   Devices are not automatically rebooted after upgrade to make the device begin running the new software version. You can select the option to reboot the device automatically after the upgrade in a later wizard page.
3. Click **Next** to continue to the next page.

   The Select Images page opens. Select a software image as described in "Selecting Software Images To Deploy" on page 36.

Selecting Software Images To Deploy

The Select Images page includes a table listing each device group and device that you selected for deployment. See Table 19 on page 37 for a description of the table columns.

If you selected the Upgrade only (Install previously staged image on device) option, only devices that contain a previously staged software image appear in the table. You cannot select a different image to install on these devices.

To select the software images to deploy, perform the following steps on the table row for each device group or individual device that you want to upgrade:

1. In the Proposed Image Version/Profile column, click **Select Image/Profile**.

   The Select Image/Profile list is displayed.
2. From the Select Image/Profile list, select a software image.

TIP: To clear this field, select **Select Image/Profile** from the list.

3. After you finish selecting software images, click **Next** to continue to the next page.

   The Select Options page opens.

TIP: A pop-up message notifies you if you do not select a software image for all the listed devices. This is just for your information. No action will be taken on devices for which you do not select a software image. In effect, this removes those devices from the job.

Select options for software deployment as described in "Selecting Options for Software Deployment" on page 37.

Table 19: Select images for devices Table

Table Column	Description
Device Family	Device family to which the device belongs. Devices are grouped by family. To display the devices within a device family, click the arrow next to the device family name.
Count	Number of devices contained within a device family.
IP Address	Device's IP address.
Device Name	Device's name.
State	Device's state: • UP—Network Director can communicate with the device. • DOWN—Network Director cannot communicate with the device.
Running Image Version	Software version the device is running.
Proposed Image Version/Profile	Software version that will be installed on the device when the job runs successfully.

Selecting Options for Software Deployment

The options that you can configure in the Select Options page are described in Table 20 on page 38. The options that are available depend on the job flow you chose in the Select Images page.

After you finish selecting options, click **Next** to continue to the next page. The Summary page opens. Review the job summary as described in "Summary of Software Deployment" on page 39.

Table 20: Image Management Job Options

Option	Action
Select Options	
All Device Types	
Delete any existing image before download	Select to delete any existing software images on devices before downloading the new software image.
Reboot device after successful installation	Select to reboot the device after the software image is installed. A reboot is required to begin running the new software version on the device. NOTE: If you want to perform a Non Stop Upgrade for an EX8200 switch (standalone and Virtual Chassis), you must select this option or manually reboot the switch after the upgrade is complete.
EX Series Only	
Check compatibility with current configuration	Select to validate the software package or bundle against the current configuration as a prerequisite to adding the software package or bundle.
Archive data (Snapshot)	Select to take an archive snapshot of the files currently used to run the switch and copy them to an external USB storage device connected to the switch.
Copy to alternate slice	Select to copy the new Junos OS image into the alternate root partition. This ensures that the resilient dual-root partitions feature operates correctly.
Non Stop Upgrade	Select if you want to perform a Nonstop software upgrade (NSSU). Nonstop software upgrade (NSSU) enables you to upgrade the software running on an EX Series switch with redundant Routing Engines or on most EX Series Virtual Chassis by using a single command and with minimal disruption to network traffic
QFabric Only	
Check compatibility with current configuration	Select to validate the software package or bundle against the current configuration as a prerequisite to adding the software package or bundle. NOTE: You can use this feature to upgrade the operating system of QFX devices to Junos OS Release 13.1 or later.
Non Stop Upgrade	Select if you want to perform a Nonstop software upgrade.
WLC Devices Only	
Use Hitless Upgrade	Select to use the hitless upgrade process to upgrade the devices. Applies only to WLC controllers in cluster mode.
Select Schedule	
Stage now	Select **Stage now** to start staging software images to devices as soon as the job runs.
Stage later time	Select **Stage later time** to schedule the staging for a later time.
Staging Schedule	If you selected Stage later time, enter the date and time for staging to start.

Table 20: Image Management Job Options *(continued)*

Option	Action
Upgrade now Upgrade later time	Select **Upgrade now** to start upgrading software images on devices as soon as staging finishes. Select **Upgrade later time** to schedule the software upgrade for a later time.
Deployment Schedule	If you selected Upgrade later time, enter the date and time for upgrade to start. If you scheduled staging, you must schedule the upgrade for at least 10 minutes after staging, to ensure that staging completes before upgrade starts.

Summary of Software Deployment

On the Summary page, review the selections you made for the job. To change selections, click **Edit** in the area that you want to change. You can also click the boxes in the process flowchart above the wizard page to navigate between pages. When you are done making selections, click **Finish** on the Summary page to save the job, and run it if you configured the job to run immediately.

Related Documentation

- Managing Software Images on page 4
- Managing Software Image Deployment Jobs on page 39
- Managing Software Images on page 33

Managing Software Image Deployment Jobs

This topic describes how to manage software image jobs. A software image job is created each time you deploy software images to devices or schedule a software image deployment. You can check the status of jobs, see job details, and cancel scheduled jobs.

To start managing software image jobs:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Image Management > View Image Deployment Jobs**.

   The Image Deployment Jobs page opens in the main window.

This topic describes:

- Selecting Software Image Management Options on page 39
- Viewing Software Image Job Details on page 40
- Using the Device Image Staging Window on page 41
- Canceling Software Image Jobs on page 41

Selecting Software Image Management Options

From the Image Deployment Jobs page, you can:

- Show deployment job details by selecting a job and clicking Show Details. See "Viewing Software Image Job Details" on page 40 for more information.
- Cancel a pending job by selecting the job and clicking Cancel Job. See "Canceling Software Image Jobs" on page 41 for more information.

Table 21 on page 40 describes the information provided in the of the Image Deployment Jobs table.

Table 21: Image Deployment Jobs Table

Table Column	Description
Job Id	An identifier assigned to the job.
Check box	Select to perform an action on the job in that row.
Job Name	Job name.
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: • CANCELLED—The job was cancelled by a user. • SCHEDULED—The job is scheduled but has not run yet. • INPROGRESS—The job is running. • SUCCESS—The job completed successfully. This state is applied if all of the devices in the job completed successfully. • FAILURE—The job failed. This state is applied if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device.
Summary	Job summary.
Scheduled Start Time	Job's scheduled start time.
Actual Start Time	Time when the job started.
End Time	Time when the job ended.
User	User who created the job.
Recurrence	This field is not used for software image management jobs.

Viewing Software Image Job Details

To view the details of a software image job:

1. Select the job in the table.
2. Click **Show Details**.

The Device Image Staging window opens. See "Using the Device Image Staging Window" on page 41 for a description of the window.

Using the Device Image Staging Window

Use the Device Image Staging window to view information about software image jobs. Table 22 on page 41 describes this window.

Table 22: Device Image Staging Window Description

Field	Description
Job Name	Job name.
Start Time	Job's scheduled start time.
End Time	Time when the job ended.
% Complete	Percentage of the job that is complete.
Status	Job status. The possible statuses are: • CANCELLED—The job was cancelled by a user. • SCHEDULED—The job is scheduled but has not run yet. • INPROGRESS—The job is running. • SUCCESS—The job completed successfully. • FAILURE—The job failed.
Host Name	Host name of device.
Status	Device status. The possible statuses are: • INPROGRESS—The job is running. • SUCCESS—The job completed successfully. • FAILURE—The job failed.
% Complete	Percentage of the job that is complete on the device.
Start Time	Time when the job started on the device.
End Time	Time when the job ended on the device.
Description	Description of the job on the device. Can include error messages for failed devices.
Close	Click to close the window.

Canceling Software Image Jobs

To cancel a software image job:

1. Select the job in the table.

2. Click **Cancel**.

Related Documentation

- Managing Software Images on page 4
- Deploying Software Images on page 35
- Managing Software Images on page 33

CHAPTER 4

Zero Touch Provisioning

Configuring and Monitoring Zero Touch Provisioning

Zero touch provisioning allows you to provision new switches in your network automatically—without manual intervention. When you physically connect a switch to a network and boot it with the factory-default configuration, the switch attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network.

The switch uses information that you configure on a Dynamic Host Control Protocol (DHCP) server to determine whether to perform these actions and to locate the necessary software image and configuration files on the network. You can configure the DHCP server by using a zero touch provisioning profile. If you do not configure a DHCP server, the switch boots with the preinstalled software and the default configuration.

The type of DHCP server that you want to use determines whether Network Director configures the DHCP server for you or whether you must manually configure the DHCP server. If you select CentOS or Ubuntu DHCP servers, Network Director configures the DHCP server by using the details that you specified in the zero touch provisioning profile. If you use any other DHCP server, you must manually configure the DHCP server. For such DHCP servers, you can use Network Director only to monitor the switches once they are provisioned. For details on configuring a DHCP server manually, see the DHCP server documentation.

For more information on zero touch provisioning for switches, see Understanding Zero Touch Provisioning.

NOTE: For detailed information about DHCP and DHCP options, see RFC2131 (http://www.ietf.org/rfc/rfc2131.txt) and RFC2132 (www.ietf.org/rfc/rfc2132.txt). These documents refers to Internet Systems Consortium (ISC) DHCP version 4.2. For more information about this version, see http://www.isc.org/software/dhcp/documentation.

Configuring Zero Touch Provisioning

Before you begin:

Ensure that the switch has access to the following network resources:

- The DHCP server that provides the location of the software image and configuration files on the network

  See your DHCP server documentation for configuration instructions.

- The File Transfer Protocol (anonymous FTP), the Hypertext Transfer Protocol (HTTP) server, or the Trivial File Transfer Protocol (TFTP) server on which the software image and configuration files are stored. If you are using an FTP server, ensure that the FTP server is configured to enable anonymous access. Refer to your FTP server documentation to know more about this.

  

  NOTE: **Although TFTP is supported, we recommend that you use FTP or HTTP instead, because these transport protocols are more reliable.**

- (Optional) A Network Time Protocol (NTP) server to perform time synchronization on the network
- (Optional) A system log (syslog) server to manage system log messages and alerts

Identify the type of DHCP server that you will be using for zero touch provisioning:

- CentOS DHCP Server—If your DHCP server uses the following command to restart the server, then select **CentOS** as the DHCP server type:

  ```
  service dhcpd restart
  ```

- Ubuntu DHCP Server—If your DHCP server uses the following command to restart the server, then select **Ubuntu** as the DHCP server type:

  ```
  service isc-dhcp-server restart
  ```

- Other—If your server is not an ISC DHCP server running on Linux operating system, then you must select **Other** and configure the DHCP server manually.

To configure zero touch provisioning:

1. While in the Deploy mode, select **Zero Touch Provisioning** > **Setup** from the Tasks pane. The Zero Touch Provisioning wizard appears.
2. Specify the server details in the Server Setup wizard page as described in "Specifying the Server Details" on page 45.

Specifying the Server Details

To configure the server settings:

1. Enter the settings described in Table 23 on page 45. Required settings are indicated in the user interface by a red asterisk (*) that appears next to the field label.

Table 23: Server Details

Field	Description
Profile Name	Name of the zero touch provisioning profile.
DHCP Server Info	
DHCP Server Type	The type of DHCP server that provides the necessary information to the switch. You can choose to configure a CentOS DHCP server, an Ubuntu DHCP server, or any other DHCP server. If you select Other, Network Director also selects the Manually Configure Server check box and hides all the other details except the File Server Details. You must configure the DHCP server manually.
Manually Configure Server	Select to indicate that you want to manually configure the DHCP server. You can configure the CentOS and Ubuntu DHCP servers manually or from Network Director. If you select Manually Configure Server check box, Network Director hides all the other details except the File Server Details.
DHCP Server	IP address or the hostname of the DHCP server.
DHCP User	Username for the DHCP server.
DHCP Password	Password for the specified username.
Confirm Password	Confirm the password.
File Transfer Server Info	
File Server	The type of file server where the software images and the configuration files are to be stored. You can choose to use an FTP, HTTP, or a TFTP file server.
File Server IP	IP address or the hostname of the file server.
File Server Root Dir	The root directory of the file server.
Optional Settings	
Syslog Server IP	IP address of the system log server, if you want to perform data logging for zero touch provisioning.
NTP Server IP	IP address of the NTP server, if you want to use time synchronization.

2. Click **Next** and proceed to specify the software image, configuration file, and the IP address range to be configured on the DHCP server. For more details, see "Specifying the Software Image and Configuration Details" on page 46.

Specifying the Software Image and Configuration Details

To specify the software image, configuration file, and the IP address range to be configured on the DHCP server:

1. Enter the password that you want to set for the root user on the switch, in the ZTP Devices Root User Password field and confirm the password in the Confirm Password field.

   

   NOTE: **Once the switch is successfully provisioned, Network Director uses this password for discovering the device.**

2. In the Configure Settings table, click **Add** to specify details for a switch model.

   Network Director adds a row to the Configure Settings table.

3. In the Device Model field, select the switch model for which you want to specify the image and configuration file details.

4. (Only for the CentOS DHCP server) In the Image File field, select the image file that you want to upload for the selected switch model. This field lists the software images that you have uploaded to Network Director from the Device Image Repository page. For details about uploading a software image, see "Managing Software Images" on page 33.

5. Do one of the following to upload the configuration file to the DHCP server:

   - Select the factory-default configuration file for the selected switch model in the Config File field. Network Director ships with a factory-default configuration for all supported switch models.
   - If you want to upload a custom configuration file for the given switch model, click **Upload Config** and select a configuration file. When you upload a custom configuration file, ensure that the configurations mentioned in "Configuration Statements for Custom Configuration of DHCP Server" on page 47 are included in the configuration file.

6. In the Subnet field, specify the subnet that the DHCP server caters to.

7. In the From IP and To IP fields, specify the range of IP addresses that the DHCP server can assign to new switches.

8. (Only for the CentOS or Ubuntu DHCP server) Click **Export DHCP Config** if you want to view the configuration that Network Director sends to the DHCP server.

   Network Director downloads the configuration and you can view it using any text editor. If you chose to configure the DHCP server manually in the Server Details page, you can use this configuration file to complete the manual configuration.

9. Click **Next** to review the details of the zero touch provisioning profile that you created.

Reviewing and Modifying Zero Touch Provisioning Settings

From this page, you can save or make changes to a zero touch provisioning profile:

- To make changes to the profile, click the **Edit** button associated with the configuration you want to change.

  Alternatively, you can click the appropriate buttons in the zero touch provisioning workflow at the top of the page that corresponds to the configuration you want to change.

  When you are finished with your modifications, click **Review** to return to this page.

- To save a zero touch provisioning profile or to save modifications to the settings of an existing profile, click **Finish**.

What To Do Next

- For manual configuration, use the DHCP configuration file to manually configure the DHCP server. If you selected the DHCP server as CentOS or Ubuntu, Network Director uploads the software image to the file server that you specified. If you selected any other DHCP server, you must manually upload the software image to the file server and specify the path when you configure the DHCP server.
- (Only for the CentOS or Ubuntu DHCP servers) For automatic configuration, Network Director configures the DHCP server with the details that you specified in the zero touch provisioning profile and uploads the software image to the file server that you specified.

Configuration Statements for Custom Configuration of DHCP Server

Insert the following configuration statements to the configuration file, if you want to upload a custom configuration file to the DHCP server:

```
system {
root-authentication {
   encrypted-password "PASSWORD"; ## SECRET-DATA
   }
}
event-options {
policy target_add_test {
   events snmpd_trap_target_add_notice;
      then {
      raise-trap;
      }
   }
}
trap-group networkdirector_trap_group {
version all;
   destination-port NDPORT;
   categories {
   link;
      services;
      authentication;
   }
```

```
    targets{
    NDIP;
    }
}
```

Monitoring Zero Touch Provisioning Profiles

You can use the Monitor ZTP Profiles page to view details about the switches that were provisioned using a given zero touch provisioning profile and added successfully to the Network Director inventory.

To monitor a zero touch provisioning profile:

1. While in the Deploy mode, select **Zero Touch Provisioning** > **Monitor** from the Tasks pane. The Monitor ZTP Profiles page appears.
2. In the Choose ZTP Profile box, select the zero touch provisioning profile that you want to monitor.

   Network Director displays the zero touch provisioning summary and details of switches that were discovered using the selected profile.

Related Documentation

- Understanding Zero Touch Provisioning in Network Director on page 14
- Managing Software Images on page 33

CHAPTER 5

Device Management

Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director

When Auto AP mode is enabled on controllers, all access points are recognized but not persistently configured on the controller. Instead, the access points are dynamically added to the controller each time the access points boot up.

NOTE: For information about enabling Auto AP mode, see *Creating and Managing Wireless Auto AP Profiles*.

You can convert access points that were dynamically added to a controller using an Auto AP profile to a persistent access point configuration on the controller. This topic describes converting dynamic access point configurations to persistent access point configurations.

To convert automatically discovered access points to persistent access points:

1. Click **Deploy** mode in the Network Director banner.
2. Under Wireless Network in the View pane, select either a controller or a cluster of controllers.
3. Click **Convert Auto AP** under Device Management in the Tasks pane.

   The Convert Auto AP page opens, displaying a list of automatically discovered access points and the information listed in Table 24 on page 50.

Table 24: Automatically Discovered Access Point Information

Field	Description
AP Number	Temporary access point number assigned by the controller.
AP Name	Temporary access point name assigned by the controller.
Model	Access point model number discovered by the controller.
Serial Number	Access point model number discovered by the controller.
IP Address	Temporary IP address assigned by the controller.

4. From the list of automatically discovered access points, select one to convert to a persistent access point, and then click **Convert Auto AP**.
5. This message is displayed: **This will convert Auto APs to configured APs. Do you want to continue?**

   Click **Yes**.

The Convert Auto AP Job details window is displayed with the converted access points.

Related Documentation

- *Understanding Auto AP Profiles*
- *Adding and Managing an Access Point*
- *Creating and Managing Wireless Auto AP Profiles*

Converting QSFP+ Ports

The 40-Gbps QSFP+ ports on QFX3500, QFX3600 and QFabric devices can be configured to operate as four 10-Gigabit Ethernet (*xe*) ports, one 40-Gigabit Ethernet (*xle*) port, or one 40-Gbps data uplink (*fte*) port (for QFabric devices).

To start converting QSFP+ ports:

1. Click **Deploy** in the Network Director banner.
2. Select the node in the View pane that contains the ports you want to convert.
3. Select the task **Device Management** > **Convert Ports**.

   The Ports Conversion wizard opens to the Device Selection page. Continue with "Selecting Devices" on page 51.

This topic describes:

Selecting Devices

Use the Device Selection page to select the devices that contain the ports you want to convert.

To select devices that contain the ports you want to convert:

1. Select the **Standalone** radio button or the **QFabric** radio button.

   The device list displays only devices of the selected type.

2. Select the devices that contain the ports you want to convert by selecting their check boxes.

3. Click **Next**.

   The Convert Ports page opens. Continue with section "Converting Ports" on page 52.

Table 25 on page 51 describes the information provided about devices on the Device Selection page. This page lists all the devices in the selected scope that contain QSFP+ ports.

Table 25: Port Conversion Device Selection Page

Column	Description
Hostname	Configured name of the device or IP address if no hostname is configured.
IP Address (Standalone devices only)	IP Address of the device.
NodeGroup Name (QFabric devices only)	Name of the node group the port belongs to.
Serial Number	Serial number on device chassis.
Platform	Model number of the device.
Connection State	Connection status of the device in Network Director: • UP—Device is connected to Network Director. • DOWN—Device is not connected to Network Director. • N/A—Connection status is unavailable to Network Director.

Table 25: Port Conversion Device Selection Page *(continued)*

Column	Description
Config State (Standalone devices only)	Displays the configuration status of the device: • In Sync—The configuration on the device is in sync with the Network Director configuration for the device. • Out Of Sync—The configuration on the device does not match the Network Director configuration for the device. This state is usually the result of the device configuration being altered outside of Network Director. You cannot deploy configuration on a device from Network Director when the device is Out Of Sync. To resolve this state, use the Resynchronize Device Configuration task in Deploy mode. • Sync failed—An attempt to resynchronize an Out Of Sync device failed. • Synchronizing—The device configuration is in the process of being resynchronized. • N/A—The device is down.

Converting Ports

Use the Convert Ports page to convert QSFP+ ports between port types.

The page contains a table in which you configure the port conversion. The Port Name (Default) column displays the default port name.

To convert QSFP+ ports:

1. To convert a port, click its **Convert to Port** column.
2. Select an option from the list that opens:
   - **No Change**—Does not change the port type.
   - **fte**—Configures the port as one 40-Gbps data uplink port (for QFabric nodes only).
   - **xle**—Configures the port as one 40-Gigabit Ethernet port.
   - **xe**—Configures the port as a group of 10-Gigabit Ethernet ports.
3. The Port Name (After Conversion) column displays what the port name will be if you commit the current settings.
4. When you finish making port type settings, click **Next**.

   The Review page opens. Continue with "Reviewing and Deploying Port Conversions" on page 52

Reviewing and Deploying Port Conversions

Use the Review page to review settings and deploy the port conversion:

1. To change settings from the Review page, click **Back** to return to previous wizard pages.
2. When you finish making changes, click **Deploy** to deploy the port conversion to the selected devices.

Related Documentation

- Understanding Deploy Mode in Network Director on page 3

Creating and Managing Node Groups

Node groups help you combine multiple QFabric Node devices into a single virtual entity within the QFabric system to enable redundancy and scalability at the edge of the data center.

To start managing nodes groups:

1. Click **Deploy** in the Network Director banner.
2. Select the fabric to manage in the network view pane.
3. Click **Manage Node Group** under Device Management in the Tasks pane.

   The Manage Node Groups page appears.

This topic describes:

- Managing Node Groups on page 53
- Creating Node Groups on page 54
- Specifying Settings for a Node Group on page 54

Managing Node Groups

Use the Manage Node Groups page to manage existing node groups and to create new ones. The configured node groups are listed in expandable and collapsible groups:

- Group: NNG—The network node group. Each fabric has only one network node group, so you cannot create another. You can edit the group's membership.
- Group: RSNG—Redundant server node groups. You can create new redundant server node groups and edit existing ones.
- Group: SNG—Server node groups. You can create new server node groups and edit existing ones.

From the Manage Node Groups page, you can:

- Create a new node group by clicking **Add**.
- Modify an existing node group by selecting it and clicking **Edit**.
- Delete a node group by selecting it and clicking **Delete**.

Table 26 on page 54 describes the information provided about node groups on the Manage Node Groups page. This page lists all node groups within the fabric that is selected in the network view.

Table 26: Manage Node Groups Information

Column	Description
Node Group Name	Name given to the node group when it was created.
Description	Description of the node group entered when it was created. TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.
Selected Nodes	Nodes that belong to the node group. The connection state of the node is indicated by an icon: The green upward pointing arrow indicates the node is connected. The red downward pointing arrow indicates the node is not connected.
Deployment State	Shows whether the node group was deployed.

Creating Node Groups

To create a node group:

1. Click **Deploy** in the Network Director banner.
2. Select the fabric to manage in the network view pane.
3. Click **Manage Node Group** under Device Management in the Tasks pane.

   The Manage Nodes Groups page appears.
4. Click **Add**.

   The Create Node Group page appears.
5. Configure the new node group as described in "Specifying Settings for a Node Group" on page 54.
6. Click **OK**.

   The node group is listed on the Manage Node Groups page with the deployment state Pending Deployment.
7. To deploy all undeployed node group changes, click **Deploy Now**.

Specifying Settings for a Node Group

Use the Create Node Group page to define the devices in the node group.

Table 27 on page 55 describes the settings available on the Create Node Group page.

Table 27: Create Node Group Settings

Field	Action
Node Group Type	Select a node group type: • SNG—Server node group. • RSNG—Redundant server node group.
Node Group Name	Type the name of the group. The following rules apply to QFabric Node group naming: • Node group names must use alphabetic (A through Z and a through z), numeric (0 through 9), or dash (-) characters. • The maximum length of a Node group name is 30 characters. • Node group names are case sensitive. For example, MY-NG-1 and my-ng-1 refer to different components. • You cannot use the reserved names **all**, **fabric**, or **director-group** as a Node group name.
Description	Type a description of the Node group, which will appear on Manage Node Groups page.
Node Selection	
Add	Click to add a device to the node group: 1. Click **Add**. 2. Select devices from the Node Device Selection page. You can select one device for a server node group, and two devices for a redundant server node group. 3. Click **OK**.
Remove	Click to remove a device from the node group: 1. Select a device from the list on the Node Device Selection page. 2. Click **Remove**.

Related Documentation

- Understanding Node Groups on page 8

Enabling or Disabling Network Ports on Switches

Network ports connect switches to the network and carry network traffic. You can enable or disable network ports of switches that are part of your network. When you enable or disable a port, the administrative status of the port changes to UP or DOWN respectively. When you disable a port, the system marks that port as administratively down, without removing the port configurations.

You can enable or disable one or more ports at a time using the Manage Port Admin State page. The status of the port is indicated by the Admin State and the Link State fields. The administrative status of a port is indicated by the Admin State field.

To enable or disable a network interface:

1. Select the device on which you want to enable or disable network interfaces, in the View pane.
2. In the Deploy mode, select **Tasks** pane > **Device Management** > **Manage Port Admin State**.

   The Manage Port Admin State page appears displaying all the physical ports available on the selected device and the current status of each port. This page also displays the port mode of each interface, if any. Port mode can be access, tagged-access, or trunk mode.
3. Do one of the following:
   - Select the check box adjacent to the ports that you want to enable and click **Change Admin State UP**.
   - Select the check box adjacent to the interfaces that you want to disable and click **Change Admin State DOWN**.
4. Click **Done**. Network Director changes the administrative status of the ports and displays a confirmation message confirming the changes.

Related Documentation

- *Understanding the Network Director User Interface*

Resynchronizing Device Configuration

A network managed by Network Director has three repositories of information about the configuration of a network device—the configuration stored on the device itself, the device configuration record maintained by Junos Space, and the Build mode configuration maintained by Network Director.

When the configuration contained in all three repositories match, the device configuration state is shown as In Sync in Network Director. When the repositories do not match, the configuration state is shown as Out of Sync. A common cause for this state is out-of-band configuration changes—that is, configuration changes made to a device outside of Network Director.

When a device state is Out of Sync, you cannot deploy configuration changes on the device in Deploy mode. Use the Resynchronize Device Configuration task to resynchronize the three configuration repositories and change the device configuration state back to In Sync.

How the Resynchronize Device Configuration task performs the resynchronization depends on the system of record (SOR) mode setting for the Junos Space Network Management Platform:

- When Junos Space is in network as system of record (NSOR) mode, the device is considered the system of record for configuration. When you resynchronize a device when Junos Space is in NSOR mode, both the Junos Space configuration record and the Network Director Build mode configuration are updated to reflect the device configuration—in other words, the out-of-band configuration changes are incorporated into both the Junos Space and the Network Director configuration repositories.
- When Junos Space is in Junos Space as system of record (SSOR) mode, you can choose whether accept or reject the out-of-band changes reflected in the device configuration. If you accept the changes, both the Junos Space configuration record and the Network Director Build mode configuration are updated to reflect the device configuration. If you reject the changes, the out-of-band changes are rolled back on the device so that the device configuration matches the Junos Space configuration record and the Network Director Build mode configuration.

For more information about out-of-band configuration changes, Junos Space SOR modes, and how Network Director resynchronizes device configuration, see "Understanding Resynchronization of Device Configuration" on page 10.

This topic covers:

The Resynchronize Device Configuration List of Devices

The Resynchronize Device Configuration page displays a list of all devices in the selected scope whose configuration was successfully imported during device discovery and whose configuration state is now Out Of Sync. You can select devices from this list and resynchronize them.

Table 28 on page 57 describes the fields in the list of devices.

Table 28: Resynchronize Device Configuration Fields

Field	Description
Name	Device hostname or device IP address.

Table 28: Resynchronize Device Configuration Fields *(continued)*

Field	Description
IP address	IP address of device.
Model	Model number of the device.
OS Version	Operating system version currently running on the device.
Connection State	Connection state: • UP—Network Director is connected to the device • DOWN—Network Director cannot connect to the device
Configuration State	Shows the configuration state of the device: • Out Of Sync—The device configuration is out of sync with either the Network Director Build mode configuration or the Junos Space configuration record or both. • Resynchronizing—The device configuration is in the process of being resynchronized. • Sync Failed—The resynchronization attempt failed. If the resynchronization is successful, the device is removed from the table.
Local Changes	Specifies whether configuration changes have been made in Build mode and are pending deployment on the device. • None—There are no configuration changes pending deployment. • View—There are configuration changes that are pending deployment. Click **View** to view the changes. These changes will be lost if you resynchronize the Build mode configuration to match the device configuration. NOTE: The Pending Changes window that appears when you click View allows you to see what profiles have been added, modified, or changed. However, because the device is not in sync, you cannot view the specific changes in CLI or XML format.
Network Changes	Indicates whether you can view the out-of-band changes: • None—The out-of-band changes are not available for viewing. You cannot view out-of-band changes in NSOR mode. In SSOR mode, you cannot view the out-of-band changes if they are already resolved in Junos Space—that is, the device configuration state in Junos Space is In Sync. • View—You can view the out-of-band changes made on the device. Click **View** to view the changes presented in XML format.

Resynchronizing Devices When Junos Space Is in NSOR Mode

To resynchronize devices when the Junos Space Network Application Platform is in NSOR mode:

1. On the Resynchronization Device Configuration page, select the device or devices that you want to resynchronize.
2. (Optional) View any pending changes to a device's configuration in Network Director by clicking **View** in the Local Changes column. These pending changes are deleted when you resynchronize the device.

3. Click **Resynchronize Configuration**.

   The Resychronize Device Configuration Results window appears. This window will be updated with status of the resynchronization when the resynchronization completes.

Resynchronizing Devices When Junos Space Is in SSOR Mode

To resynchronize devices when the Junos Space Network Management Platform is in SSOR mode:

1. On the Resynchronization Device Configuration page, select the device or devices that you want to resynchronize.
2. (Optional) View any pending changes to a device's configuration in Network Director by clicking **View** in the Local Changes column. These pending changes are deleted if you accept the out-of-band changes when you resynchronize the device.
3. (Optional) View the out-of-band configuration changes by selecting **View** in the Network Changes column. If you accept the out-of-band changes when you resynchronize the device, these changes will be reflected in the Build mode configuration. If you reject the out-of-band changes when you resynchronize the devices, these changes will be deleted from the device. For more information about viewing the out-of-band changes, see "Viewing the Network Changes" on page 60.

   

   NOTE: **Out-of-band changes that were made with the Junos Space configuration editor or that were already accepted in Junos Space are not shown. Such changes also cannot be rejected.**

4. Click **Resynchronize Configuration**.
5. In the Confirm dialog box:
   - Click **Accept device changes** if you want to accept the out-of-band changes.
   - Click **Reject device changes** if you want to reject the out-of-band changes and have the configuration that existed on the device before the out-of-band changes were made be reinstated.

   click **Submit**.

   The Resychronize Device Configuration Results window appears. This window will be updated with status of the resynchronization when the resychronization completes.

NOTE: **Device changes made by the Junos Space configuration editor or device changes that have been accepted in Junos Space cannot be rejected. Even if you select Reject device changes, these changes will not be rejected and instead will be incorporated into the Build mode configuration.**

Viewing the Network Changes

The Network Changes window shows the out-of-band configuration changes made to a device when Junos Space is in SSOR mode.

Not all out-of-band configuration changes are shown in this window. Configuration changes are shown only when the device configuration differs from the Junos Space configuration record—that is, when the device configuration state in Junos Space is not In Sync. For example, if the out-of-band changes were deployed from the Junos Space configuration editor or if the out-of-band changes were already accepted in Junos Space, the configuration changes will not appear in this window.

The configuration changes are shown in XML format. If there have been multiple out-of-band changes—that is, there has been more than one configuration commit, or save, on the device—the changes are grouped by each commit.

The following information is provided for each configuration commit:

- junos:commit-seconds—Specifies the time when the configuration was committed as the number of seconds since midnight on 1 January 1970.
- junos:commit-localtime—Specifies the time when the configuration was committed as the date and time in the device's local time zone.
- xmlns:junos—Specifies the URL for the DTD that defines the XML namespace for the tag elements.
- junos:commit-user—Specifies the username of the user who requested the commit operation.

Viewing Resynchronization Job Status

The Resychronize Device Configuration Results window appears after you start a resynchronization job. This window is automatically updated with the resynchronization status for each device when the job completes.

You can also view the status of the resynchronization jobs using the Manage Jobs task in System mode. The following jobs are associated with resynchronization:

- Resynch Network Elements—This job runs in NSOR mode and resynchronizes the Junos Space configuration record with the device configuration.
- Resolve OOB Changes—This job runs in SSOR mode and resolves the out-of-band changes for Junos Space—either accepting the changes and updating the Junos Space configuration or rejecting the changes and rolling back the changes on the device.
- Resynchronize devices—This job runs in both NSOR and SSOR mode and resynchronizes the Build mode configuration with the device configuration.

Related Documentation

- Understanding Resynchronization of Device Configuration on page 10
- *Managing Jobs*

Viewing a Device's Current Configuration from Network Director

You can view a device's current configuration from Network Director. This is a convenient way to view device configurations without leaving Network Director.

To view a device's current configuration:

1. Click **Build** or **Deploy** in the Network Director banner.
2. Select the device in the View pane.
3. Select **Device Management > Show Current Configuration** in the Tasks pane.
4. The device's current configuration displays in the main window.

Related Documentation

- *Understanding the Network Director User Interface*
- *Understanding the Build Mode Tasks Pane*

CHAPTER 6

Configuration File Management

Managing Device Configuration Files

You can back up device configuration files to the Network Director server. You can perform several actions on backed up configuration files, such as restoring configuration files to devices, and viewing and comparing configuration files.

To start managing device configuration files:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Device Configuration Files > Manage Device Configuration Files**.

   The Manage Device Configuration page opens in the main window. The table lists the devices that have configuration files backed up.

This topic describes:

Selecting Device Configuration File Management Options

From the Manage Device Configuration page, you can:

- Back up device configuration files by clicking Backup. See "Backing Up Device Configuration Files" on page 64 for more information.
- Restore backup device configuration files to devices by selecting devices and clicking Restore. See "Restoring Device Configuration Files" on page 65 for more information.

- View backed up configuration files by selecting a device and clicking View Configuration File. See "Viewing Device Configuration Files" on page 65 for more information.
- Compare backed up device configuration files by selecting devices and clicking Compare Config Files. See "Comparing Device Configuration Files" on page 65 for more information.
- Delete backup device configuration files by selecting devices and clicking Delete. See "Deleting Device Configuration Files" on page 66 for more information.

Table 29 on page 64 describes the information provided in the Manage Device Configuration table.

Table 29: Manage Device Configuration Table

Table Column	Description
Device Name	Device name.
Config File Version	Version number of the backup configuration file.
First Backup on	Date when the oldest version of the backup configuration file was created.
Most Recent Backup on	Date when the configuration file was backed up most recently.

Backing Up Device Configuration Files

To back up device configuration files:

1. Click **Backup**.

   The Backup Devices Configuration page opens in the main window.

2. Select the devices to back up from the device tree.
3. To back up configuration files immediately, click **Backup Now**.

   The backup job runs. When it finishes, the Manage Device Configuration table shows updated information for the devices you backed up.

4. To schedule the backup to run later, click **Schedule Backup**.

   The Schedule Backup window opens.

   a. Select the **Schedule at a later time** check box.

   b. Specify when the backup will run using the **Date and Time** fields.

   c. Optionally, configure the backup job to repeat by selecting the **Repeat** check box, then specifying the backup schedule using the provided fields.

      Optionally, you can specify when repeated backups will stop by selecting the **End Time** check box, then specifying the last date on which the repeated backup job will run using the **Date and Time** fields.

   d. Click **Schedule Backup**.

Restoring Device Configuration Files

You can restore a backed up configuration file to the device from which it was backed up.

CAUTION: Restoring a configuration file to a device is considered an out-of-band configuration change, which can cause some unexpected results. For more information, see *Understanding Build Mode in Network Director*.

To restore backed up configuration files to devices:

1. Select the devices to restore from the Manage Device Configuration list.
2. Click **Restore**.

   The Restore Device Configuration File(s) window opens.
3. To restore a configuration file that is older than the most recent version, click in the **Latest Version** cell and select the version to restore.
4. Click **Restore**.

Viewing Device Configuration Files

To view the backed up configuration files for a device:

1. Select the device from the Manage Device Configuration list.
2. Click **View Configuration File**.

   The Device Configuration Summary window opens, displaying the most recently backed up configuration file.
3. To view an older stored configuration file version, select a version number from the **Config File Version** list.

Comparing Device Configuration Files

To compare backed up device configuration files:

1. Select the configuration files to compare from the Manage Device Configuration list.
2. Click **Compare Configuration Files**.

   The Compare Configuration Files window opens.
3. Select a source device from the **Source Device** list and a configuration file version from the **Config File Version** list.

4. Select a target device from the **Target Device** list and a configuration file version from the **Config File Version** list.
5. The configuration file versions you selected are displayed in the window. The file name and version appears at the top of each file. The differences between the configuration files are color-coded. The color-coding legend appears at the top of the window.

Deleting Device Configuration Files

When you delete a device's backed up configuration, all of the configuration file versions for the device are deleted.

To delete device configuration files:

1. Select the configuration files to delete from the Manage Device Configuration list.
2. Click **Delete**.

   The Delete Device Configuration File(s) window opens.
3. Verify that the correct devices are listed, then click **Delete**.

Managing Device Configuration File Management Jobs

Each time you back up or restore device configuration files, a device configuration file management job is created.

To manage device configuration file management jobs:

1. Click **Deploy** in the Network Director banner.
2. In the Tasks pane, select **Device Configuration Files > View Configuration File Mgmt Jobs**.

   The Device Configuration Jobs page opens in the main window, listing the device configuration file management jobs.

Managing these jobs is similar to managing other types of jobs using the System mode. The advantage of accessing the jobs this way is that the jobs list show only configuration file management jobs. See *Managing Jobs* for more information.

Related Documentation

- Understanding the Deploy Mode Tasks Pane on page 6
- Understanding Deploy Mode in Network Director on page 3
- *Managing Jobs*