JUNIPER NETWORKS | Engineering Simplicity

Junos ® Space Network Director

FIPS Evaluated Configuration Guide for Network Director

Published
2021-02-18

Release
3.6

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® Space Network Director FIPS Evaluated Configuration Guide for Network Director
3.6
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

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 https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | vii

Documentation and Release Notes | **vii**

Documentation Conventions | **vii**

Documentation Feedback | **x**

Requesting Technical Support | **x**

- Self-Help Online Tools and Resources | **xi**
- Creating a Service Request with JTAC | **xi**

1 **Overview**

Understanding Network Director in FIPS Mode | 13

- About the Cryptographic Boundary on Network Director | **13**
- How FIPS Mode Differs from Non-FIPS Mode | **14**
- Validated Version of Network Director in FIPS Mode | **14**

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 14

- FIPS Terminology | **15**
- Supported Cryptographic Algorithms | **15**
- Weak Digital Certificates | **17**

Understanding the Network Director User Interface | 18

- Network Director Banner | **19**
- View Pane | **22**
  - Displaying Devices in Various Network Views | **22**
  - Filtering the Network Tree | **23**
  - Expanding or Collapsing Nodes in the Network Tree | **24**
  - Searching the Network Tree | **24**
- Tasks Pane | **25**
- Alarms | **26**
- Main Window or Workspace | **26**
- Tables in Network Director | **27**
  - Moving and Resizing Columns | **27**
  - Displaying the Column Drop-Down Menu | **27**

Sorting on a Column | 28

Hiding and Exposing Columns | 28

Searching Table Contents | 29

Filtering Table Contents | 31

Setting up a Junos Space Appliance for Network Director | 31

Setting Up User and System Preferences | 32

Accessing the Preferences Page | 33

Choosing Server Time or Local Time | 34

Specifying Search Preferences | 34

Enabling Import of Configuration Group Data from Ethernet Design | 34

Specifying the Open Clos Server URL | 35

Selecting the Approval Mode | 35

Setting up Auto-resynchronization Preferences | 36

Retaining Network Director Reports | 37

Specifying Wireless Preferences | 37

Changing Monitor Mode Settings | 37

Disabling Data Collection for Monitors | 38

Changing the Polling Interval | 40

Enabling and Disabling Collection for Managed Devices | 41

Specifying Database History Retention | 42

Specifying the Data Learning Engine (DLE) Settings | 42

Changing Alarm Settings | 44

Configuring Global Alarm Notifications | 44

Retaining Alarm History | 45

Specifying Event History | 45

Enabling Alarms | 45

Changing the Severity of Individual Alarms | 59

Configuring Threshold Alarms | 59

Configuring Individual Alarm Notifications | 59

Modifying Data Center Synchronization Interval Using the Virtualization Tab | 60

2 Understanding Roles and Authentication Methods

Understanding Roles and Services for Network Director in FIPS Mode | 62

Understanding Password Specifications and Guidelines for Network Director in Junos Space in FIPS Mode | 63

3 Deploying Network Director

Installing Network Director | 66

- Installing Network Director From Junos Space Store | 66
- Installing Network Director by Manually Downloading the Network Director Application Image | 67
- Discovering Devices | 69

Installing Hot Patch | 71

Logging In to Network Director | 71

4 Working in Build Mode

Discovering Devices in a Physical Network | 73

- Specifying Target Devices | 74
- Specifying Discovery Options | 76
- Specifying Schedule Options | 78
- Reviewing Device Discovery Options | 78
- Viewing the Discovery Status | 79

Managing the Topology View | 80

- Viewing the Network Topology | 81
- Refreshing the Topology | 83
- Viewing Topology | 84
- Viewing Topology Discovery Job | 85
- Setting Up Locations | 86
- Viewing the Alarm Details | 86
- Discovering the Linux Hosts | 86
- Displaying Device Connectivity | 87
- Displaying QFabric Connectivity | 91
- Displaying Virtual Chassis and Virtual Chassis Fabric Connectivity | 94
- Displaying Virtual Network Connectivity | 97

Displaying Third-Party Device Details | **97**

Uploading Floor Plans | **98**

Uploading Topology Map | **99**

5 **Configuring Cloud-Based Datacenter Networks**

Creating Data Centers Using Network Director | 101

Create a Data Center | **101**

View the Data Center Creation Status | **104**

Assigning Network Devices to a Data Center | **106**

6 **Working with Aruba Devices and Applications in Network Director**

Linking to the Aruba Airwave Application | 108

7 **Importing RingMaster Data**

Importing RingMaster Data to Network Director | 110

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vii
- Documentation Conventions | vii
- Documentation Feedback | x
- Requesting Technical Support | x

Use this guide to operate Network Director in Federal Information Processing Standards (FIPS) 140-2 Level 1 environment. FIPS 140-2 defines security levels for hardware and software that perform cryptographic functions.

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 https://www.juniper.net/documentation/.

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 https://www.juniper.net/books.

Documentation Conventions

Table 1 on page viii 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page viii 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*

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

Convention	Description	Examples
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)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (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)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies 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		

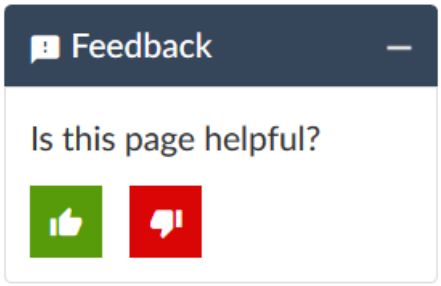
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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 https://support.juniper.net/support/requesting-support/.

CHAPTER 1

Overview

Understanding Network Director in FIPS Mode | 13

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 14

Understanding the Network Director User Interface | 18

Setting up a Junos Space Appliance for Network Director | 31

Setting Up User and System Preferences | 32

Understanding Network Director in FIPS Mode

IN THIS SECTION

- About the Cryptographic Boundary on Network Director | 13
- How FIPS Mode Differs from Non-FIPS Mode | 14
- Validated Version of Network Director in FIPS Mode | 14

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, Network Director complies with the FIPS 140-2 Level 1 standard.

Operating Network Director in a FIPS 140-2 Level 1 environment requires enabling FIPS mode in Junos Space. If FIPS mode is enabled in Junos Space, then Network Director automatically supports FIPS mode.

For regulatory compliance information about FIPS for Juniper Networks products, see the Juniper Networks Compliance Advisor.

About the Cryptographic Boundary on Network Director

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. Junos Space in FIPS mode prevents the cryptographic module from executing any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module by, for example, being displayed on a console or written to an external log file.

Cryptographic boundary is determined by different configurations. For example, you can configure Junos Space with Network Director or Junos Space with Security Director and Network Director.

How FIPS Mode Differs from Non-FIPS Mode

Unlike Junos Space Network Director in non-FIPS mode, Junos Space Network Director in FIPS mode is a *non-modifiable operational environment*. In addition, Junos Space Network Director in FIPS mode differs in the following ways from Junos Space in non-FIPS mode:

- Self-tests of all cryptographic algorithms are performed at Junos Space startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and Message Digest 5 (MD5) are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters.

Validated Version of Network Director in FIPS Mode

To determine whether a Junos OS Evolved release is FIPS 140-2 1 or FIPS 140-3 1 certified, see the compliance page on the Juniper Networks Web site (https://apps.juniper.net/compliance/fips.html).

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- FIPS Terminology | **15**
- Supported Cryptographic Algorithms | **15**
- Weak Digital Certificates | **17**

Use the definitions of FIPS terms and supported algorithms to help you understand Network Director in FIPS mode.

Network Director uses the user administration features of the Junos Space platform on which it runs. Use Junos Space for tasks such as adding, deleting, and editing user accounts and roles, and changing user passwords. Refer to the Junos Space documentation for information about user administration.

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects.

Cryptographic module—The set of software that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Super Administrator—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos Space Network Director in FIPS mode. For details, see *Understanding Roles and Services for Junos Space in FIPS Mode*.

FIPS—Federal Information Processing Standards. FIPS 140-2 specifies requirements for security and cryptographic modules. Junos Space Network Director in FIPS mode complies with FIPS 140-2 Level 1.

SSH—A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for **rlogin**, **rsh**, and **rcp** in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos Space, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.

Supported Cryptographic Algorithms

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

> **BEST PRACTICE:** For FIPS 140-2 compliance, use only FIPS-approved cryptographic algorithms in FIPS mode.

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods use different keys for encryption and decryption.

AES—The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.

Diffie-Hellman—A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method—keys are typically used only for a short time, discarded, and regenerated.

ECDH—Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA uses the P-256, P-384, and P-521 curves that can be configured under OpenSSH.

HMAC—Defined as "Keyed-Hashing for Message Authentication" in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos Space in FIPS mode, HMAC uses the iterated cryptographic hash functions SHA-1, SHA-256, and SHA-512 along with a secret key.

SHA-256, SHA-384, and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

3DES (3des-cbc)—Encryption standard based on the original Data Encryption Standard (DES) from the 1970s that used a 56-bit key and was cracked in 1997. The more secure 3DES is DES enhanced with three multiple stages and effective key lengths of about 112 bits. For Junos Space in FIPS mode, 3DES is implemented with cipher block chaining (CBC).

The following Table 3 on page 16 indicates supported algorithms for Network Director in Junos Space:

Table 3: Supported Algorithms for Network Director in Junos Space

Protocol	Key Exchange	Authentication	Encryption	MAC	Cipher
TLSv1.2	DH	RSA	AESGCM(128)	AEAD	DHE-RSA-AES128-GCM-SHA256
TLSv1.2	DH	RSA	AES(128)	SHA256	DHE-RSA-AES128-SHA256
TLSv1.2	DH	RSA	AESGCM(256)	AEAD	DHE-RSA-AES256-GCM-SHA384

Table 3: Supported Algorithms for Network Director in Junos Space *(continued)*

Protocol	Key Exchange	Authentication	Encryption	MAC	Cipher
TLSv1.2	DH	RSA	AES(256)	SHA256	DHE-RSA-AES256-SHA256
TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD	ECDHE-RSA-AES128-GCM-SHA256
TLSv1.2	ECDH	RSA	AES(128)	SHA256	ECDHE-RSA-AES128-SHA256
TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD	ECDHE-RSA-AES256-GCM-SHA384
TLSv1.2	ECDH	RSA	AES(256)	SHA384	ECDHE-RSA-AES256-SHA384

Network Director in Junos Space supports the following third party cryptographic modules, which are FIPS compliance:

- Linux Kernel Crypto
- OpenSSL
- GnuTLS
- Libgcrypt
- Network Security Services
- JDK JCE
- Bouncy Castle

Weak Digital Certificates

Enable the following services only with HTTPS TLSv1.2 configured with SHA256 RSA 2048 signature:

- Data Center
- DLE
- Aruba Airwave
- Ring Master

Understanding the Network Director User Interface

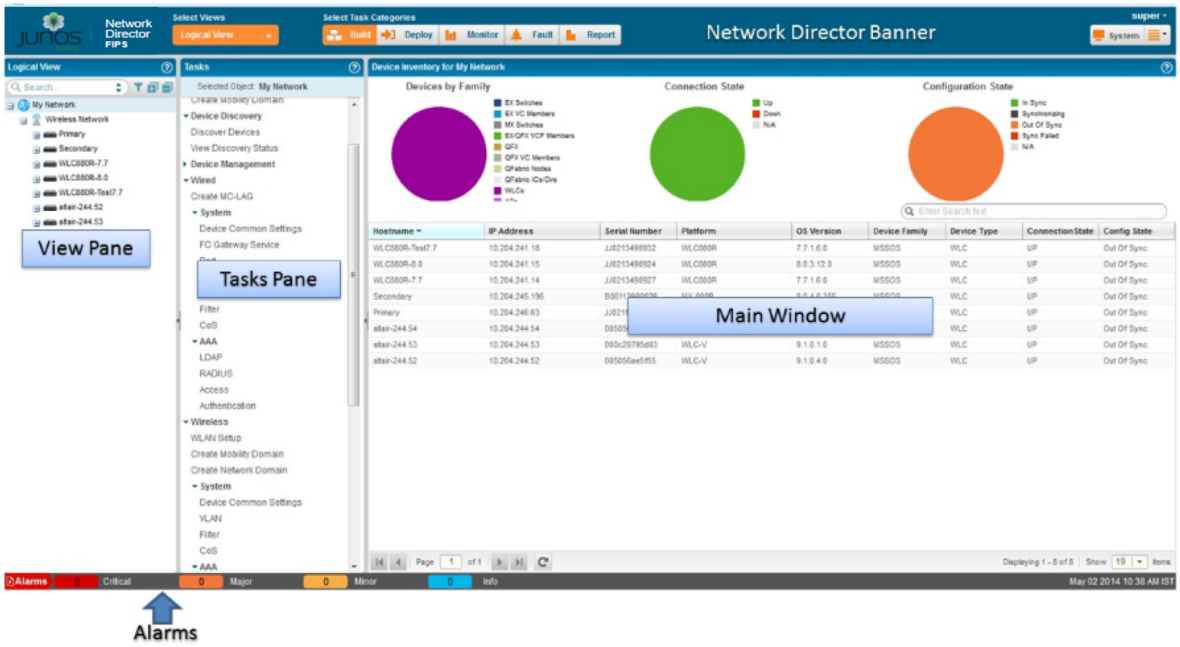
IN THIS SECTION

- Network Director Banner | 19
- View Pane | 22
- Tasks Pane | 25
- Alarms | 26
- Main Window or Workspace | 26
- Tables in Network Director | 27

Junos Space Network Director in FIPS mode provides a simple to use, HTML5-based, Web 2.0 user interface that you can access through standard Web browsers. The user interface is task-oriented, using task-based workflows to help you accomplish administrative tasks quickly and efficiently. It provides you the flexibility to work with single devices or with multiple devices grouped by logical relationship, location, or device type. You can filter, sort, and select columns in tables, making looking for specific information easy.

Figure 1 on page 19 illustrates the main components of the interface.

Figure 1: The Network Director User Interface Components



This topic describes:

Network Director Banner

Use the Network Director banner, shown in Figure 2 on page 20, to select the working mode. You can also use the Network Director banner to perform other global tasks, such as setting up your preferences or accessing Junos Space. Table 4 on page 20 describes the functions available to you on the banner.

Figure 2: Network Director Banner

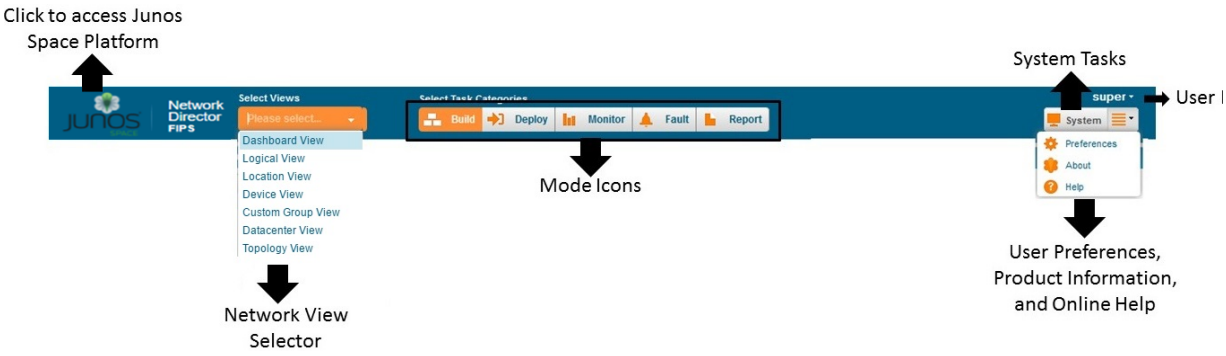


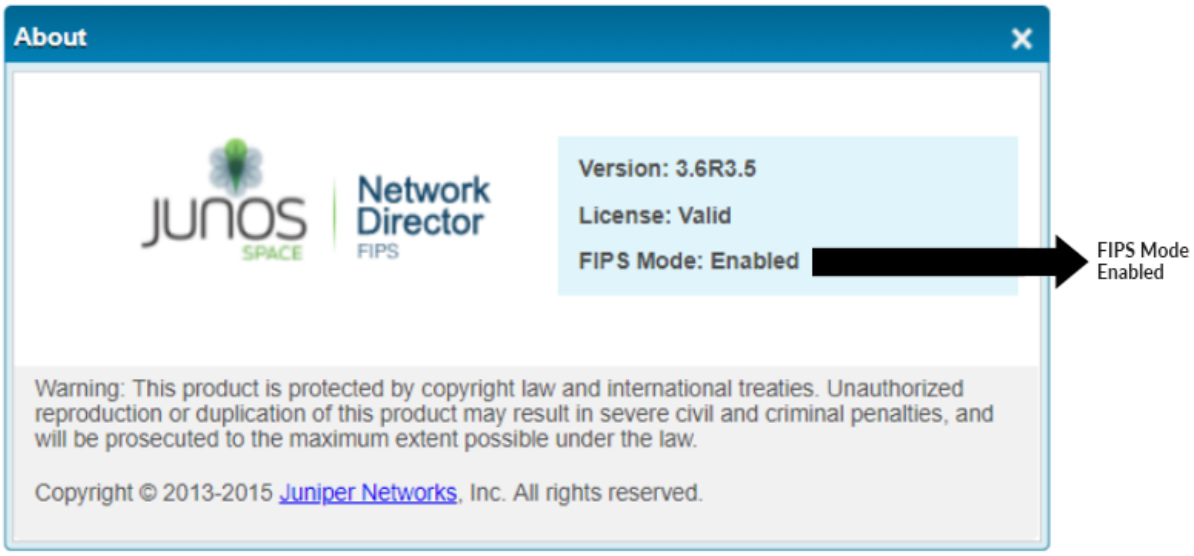
Table 4: Network Director Banner Functions

Item	Function
Accessing Junos Space Platform	Click to exit Network Director and open the Junos Space Network Application Platform. You can switch back and forth between Network Director and Junos Space without logging in again.
Network View Selector	Select the network view that you want to work in. You can choose from one of the following views: • Dashboard View • Logical View • Location View • Device View • Custom Group View • Datacenter View • Topology View For more details, see "Displaying Devices in Various Network Views" on page 22.
Mode Icons	Select the mode you want to work in. **NOTE:** You might not have access to all the Network Director modes. What modes you have access to depends on your assigned user role.
User Log out	Displays the username using which you logged in to Network Director. Click the Down arrow next to the username and select Logout to log out of Network Director and Junos Space.

Table 4: Network Director Banner Functions *(continued)*

Item	Function
System Tasks	Access the system tasks such as viewing audit logs, jobs, and to collect troubleshooting logs. Click the Down arrow next to System and select Preferences to set your Network Director user and system preferences.
System Preferences, Product Information, and Online Help	Click this button and select an appropriate option: • Preferences—Enables you to set your Network Director user and system preferences. • Help—Open searchable help. This help icon is not context-sensitive—it always opens help to the first page. From here, you can browse or search the help. Context-sensitive help is available from the help icon provided on each pane or page. • About—Figure 3 on page 21 displays information about Network Director, such as the currently running version and FIPS mode.

Figure 3: FIPS Mode Enabled



In addition to this, Network Director displays the date and time in the local time zone in the bottom right corner.

View Pane

IN THIS SECTION

- Displaying Devices in Various Network Views | 22
- Filtering the Network Tree | 23
- Expanding or Collapsing Nodes in the Network Tree | 24
- Searching the Network Tree | 24

In the View pane, Network Director provides you a unified, hierarchal view of your wired, wireless, and data center networks in the form of a expand tree that is expandable and collapsible. By selecting both a view and a node in the tree, you indicate the *scope* over which you want an operation or task to occur. For example:

- By selecting the Access node in Logical View, you indicate that the scope for a task is all access switches under the Access node.
- By selecting a floor node in Location View, you indicate that the scope for a task is all devices belonging to that floor.
- By selecting the EX4200 node in Device View, you indicate that the scope for a task is all EX4200 switches in your network.

You can perform the following actions in the View pane:

Displaying Devices in Various Network Views

Use the selection box in the Network Director banner to choose one of the following network views:

- Dashboard View—This is a is a customizeable view that provides information about your network, and is the default view that opens when you log in. You can select and add monitoring widgets to the Dashboard View based on your requirements. This is the default view that opens when you log in to Network Director.
- Logical View—Devices are organized by their logical relationships in the network. All switches appear in the Switching Network and are categorized by their role in the network: access, aggregation, or core. All wireless devices appear in the Wireless Network. Controllers appear under the mobility domains to which they belong and access points appear under the controller or cluster that manages them. All QFX Series switches that are part of a QFabric appear in the Fabric node.

  Network Director builds most of this view for you as you discover devices. However, you need to manually assign switches to the access, aggregation, or core categories.

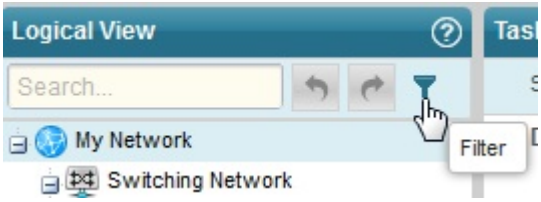
- Location View—Devices are organized by their physical locations. You build this view by creating sites, building, floors, aisles, racks, outdoor areas, and then assigning your switches, wireless controllers, access points, and QFabric systems to these locations.
- Device View—Devices are organized by device type: switches, wireless LAN controllers, and QFabric systems. Within each device type, devices are organized by device model. For example, all models of EX4200 switches are grouped together under one node in the tree.
- View—Displays devices that are part of your network
- Custom Group View—If you have defined one or more custom groups, Network Director displays these custom groups in this view. You can manually add devices to a custom group or define a rule to automatically add devices to the custom group once they are discovered in Network Director. The devices are grouped under each custom group.
- Topology View—Topology enables you to view all the discovered devices in your network, overlaid on a map where the devices are located across sites, buildings, floors, closets, aisles, and racks along with their physical interconnection with other devices in your network. Topology also provides visualization around physical and logical connectivity between various discovered interconnected devices.
- Datacenter View—Datacenter view enables you to view all the data centers in Network Director. Expand each data center to view servers that are part of the data center,

Filtering the Network Tree

To make it easier for you to focus on selected aspects of your network, you can apply predefined filters to your network tree so that only nodes and devices that meet the filter criteria are shown. For example, you can apply a filter so that only devices in a specific building are shown in the network tree in all views.

To apply filters:

1. Click the filter icon:



2. In the Filters dialog box, click **Show available filters**.

   The Available Filters section of the dialog box appears.

3. Under Available Filters, click the tab for the view you want to use to define your filter. For example, if you want to filter on devices—that is, show only certain types of devices–click the **Device** tab.

   The filters that you can apply are listed below the tab.

4. To select a filter, click its associated plus icon.

   The filter appears in the Selected Filters section of the dialog box. You can repeat Steps 3 and 4 until you have selected all the filters you want apply.

5. Click **Apply**.

   The Filters dialog box closes and the filters are applied. The filter icon changes appearance to indicate that filters have been applied:

To remove a filter, click the filter icon, click the trash can next to the filter in the Selected Filters list, and click **Apply**.

Expanding or Collapsing Nodes in the Network Tree

To expand a node in the network tree, select the node and then click the **Expand All** icon:

The node you selected and any child nodes under the selected node are expanded to show their contents.

Similarly, to collapse a node in the network tree, select the node and then click the **Collapse All** icon (next to the Expand All icon). The node you selected is collapsed and no nodes under it are shown.

Searching the Network Tree

To quickly find and select a device or device group, use the search function.

To perform a search, type three or more characters into the Search box and click the **Search** icon, as shown in Figure 4 on page 25.

Figure 4: Performing Search in the View pane

Network Director finds the first instance of a node whose name contains the characters. To find the next instance, click the right arrow.

Searches are not case-insensitive: a search on *wla115* and one on *WLA115* return the same results.

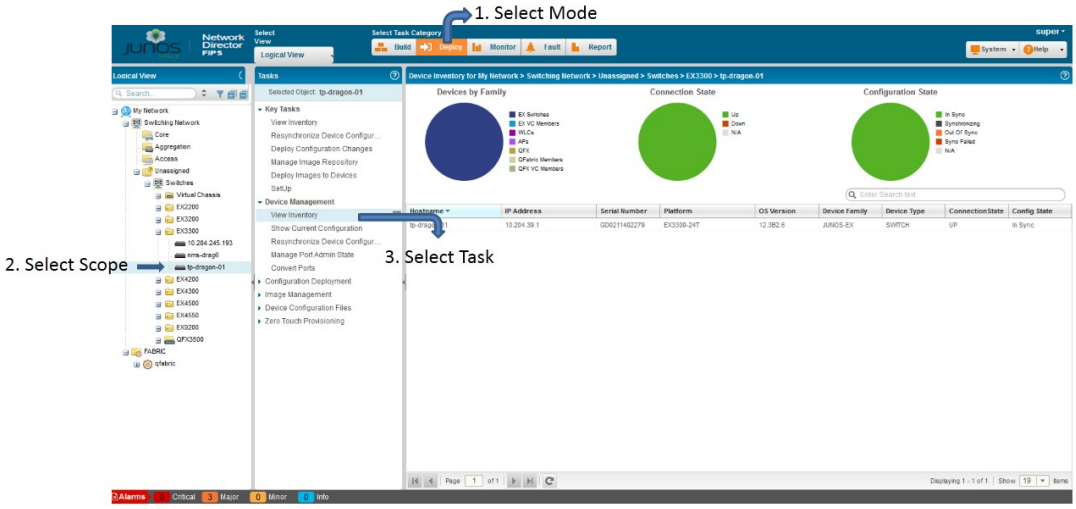
Tasks Pane

The Tasks pane is available in every mode and lists tasks specific to that mode. In addition to changing according to the mode selected, tasks listed in the Tasks pane can change as you select different scopes in the View pane. For example, some tasks are appropriate only at the device level and thus appear only when you have selected an individual device.

Clicking a task brings up task-specific content in the main window.

In general, to perform a task in Network Director, you navigate to the task as shown in Figure 5 on page 25. You select your mode, your scope, and then your task.

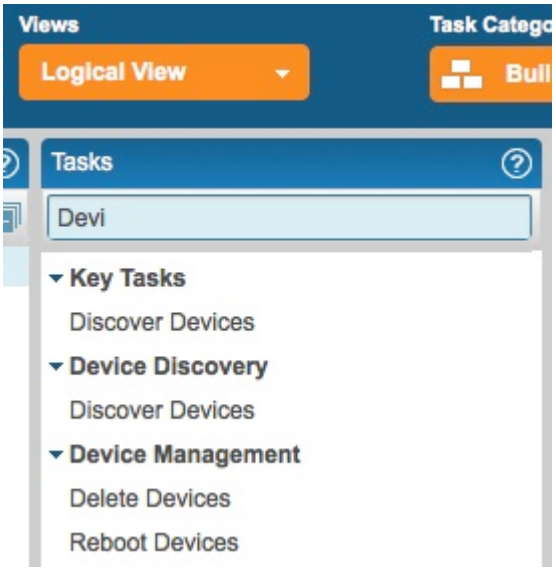
Figure 5: Navigating to a Task in a Tasks Pane



TIP: The location of the Tasks pane changes with mode. In Build and Deploy mode, it is adjacent to the View pane. In Monitor, Fault, and Report mode, it located to the right of the main window.

Use the Search box in the Tasks pane to easily locate a task, as shown in Figure 6 on page 26. To perform a search, type three or more characters into the Search box and press Enter.

Figure 6: Performing Search in the Tasks pane



Alarms

The Alarms bar that is displayed at the bottom of your browser window provides a quick summary of how many critical, major, minor, and info alarms are currently active in the network and is visible in every mode. To display more information about alarms, click the alarm count or the Alarms banner. You are automatically placed in Fault mode and the Fault mode monitors are displayed.

Main Window or Workspace

The main window or workspace displays the content relevant to the mode, scope, and task you have selected. When you log in to Network Director, this pane displays the Device Inventory page. The Device Inventory page is the default landing page for Build and Deploy modes. It contains a list of the devices for

your current scope. It includes pie charts that permit you to see at a glance the connection states, configuration synchronization states, and device-type distribution for your devices.

Tables in Network Director

IN THIS SECTION

- Moving and Resizing Columns | 27
- Displaying the Column Drop-Down Menu | 27
- Sorting on a Column | 28
- Hiding and Exposing Columns | 28
- Searching Table Contents | 29
- Filtering Table Contents | 31

Tables are used throughout Network Director to display data. These tables share common features. By becoming familiar with these features, you can navigate and manipulate tabular data quickly and efficiently. The following sections describe:

Moving and Resizing Columns

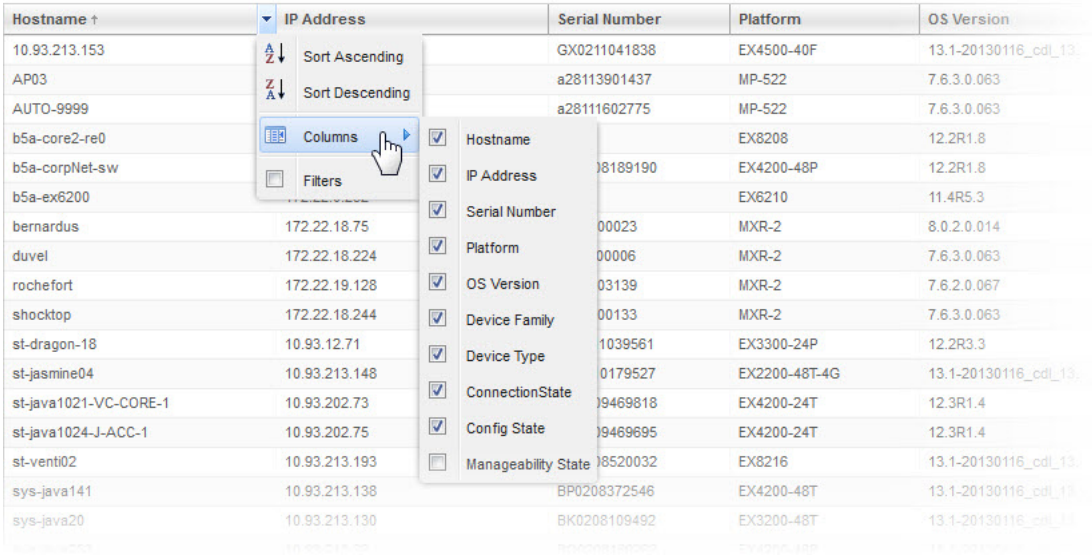
You can reposition and resize columns in a table. To move a column, drag and drop the column head to the new location. Network Director displays a green check mark when you mouse over a valid column location.

To resize a column, mouse over the edge of a column until the cursor becomes two vertical lines with outward arrows. Drag the column width to the new size.

Displaying the Column Drop-Down Menu

A drop-down menu is available from each column head, allowing you to perform additional operations on columns. To display the column drop-down menu, mouse over the column head. A downward arrow appears. By clicking the arrow, you display the drop-down menu, as shown in Figure 7 on page 28.

Figure 7: Column Drop-Down Menu



Sorting on a Column

You can sort the table on a column by clicking the column head—each click changes the direction of the sort. In addition, you can use the Sort Ascending and Sort Descending options in the drop-down menu.

When you sort on a column, a small arrow appears next to the column name to indicate that the table is being sorted by the column and the direction of the sort.

Network Director uses a lexical sort for tabular data that is not strict numeric data, which means that data such as IP addresses do not sort in numerical sequence, as shown in Table 5 on page 28.

Table 5: Numerical Sorts and Lexical Sorts

Numerical Sort	Lexical Sort
10.93.200.65	10.93.200.129
10.93.200.129	10.93.200.199
10.93.200.199	10.93.200.65

Hiding and Exposing Columns

You can customize your tables by hiding or exposing columns. This way, you can choose to see only relevant information.

To hide or expose columns, display the drop-down menu for any column head and mouse over the Columns option, as shown in Figure 7 on page 28. Select a column to expose it—clear a column to hide it.

As a general rule, Network Director displays all columns in a table by default. However, some tables have more columns than can fit easily within the page. In these tables, some columns are hidden by default.

Searching Table Contents

You can search for specific data in large tables by using search criteria.

To search for an item in a table, enter the search term in the text box. Select ANY for Network Director to search for the term in all columns in the table. Every table has a predefined default column that the system searches first; before it proceeds to search other columns.

You can also choose to search a particular column for a term. Network Director displays a list of all the columns in a table. To search a particular column for a term, select that column for the list.

NOTE: When you enter a search expression, note the following:

- You must add a back slash "\" if you want to use the following special characters in the search text:

  + ~ && || ! ( ) { } [ ] ^ " ~ * ? : \

- Field names are case-sensitive.

  For example, if you have a few systems running on Junos OS 12.3 Release 4.5, then os: 12.3R4.5 returns search results, whereas OS: 12.3R4.5 does not return search results. This is because the field name that is indexed is *os* and not *OS*.

- If you want to search for a term that includes a space, enclose the term within double quotation marks.

  For example, to search for all devices that are synchronized (that is, In Sync), enter "In Sync" in the Search field.

- You must append "*" if you want to search using partial keywords. Otherwise, the search returns 0 (zero) matches or hits.

You can filter search results by specifying one or more search terms. Network Director uses the AND operator for each search term that you enter. Network Director lists the search results in the table, depending on the search criteria that you specified.

For example, perform the following steps to search for an EX4200 switch that is running Junos OS Release 12.2:

1. Enter **EX4200** as the search term in the text box.

2. From the list that appears, select to search the Platform column.

   Network Director lists all the EX4200 switches in your network.

3. Enter **12.2** as the search term after the comma separator in the text box.

4. From the list, select to search from the OS Version column.

Network Director lists all the EX4200 switches in your network that are running Junos OS Release 12.2.

Filtering Table Contents

For large tables, it is helpful to be able to sort data to show only relevant entries. When you mouse over the Filters option in the column drop-down menu, a fill-in box appears where you can type filter criteria. If you type a text string and click **Go**, entries that do not contain the text string (filter criterion) are removed from the table. A red asterisk appears on the column head to indicate that the column has been filtered. To restore all entries to the table, clear the Filters option.

For example, to filter the Device Inventory page so that only devices in the **192.168.1.0** subnet are displayed:

1. Mouse over the right side of the IP Address column head to expose the downward arrow.
2. Click the arrow to display the column drop-down menu.
3. Mouse over **Filters** to display the Filter field.
4. Type **192.168.1.** in the field and click **Go**.

Only the devices in the **192.168.1.0** subnet are shown.

Setting up a Junos Space Appliance for Network Director

The following management interfaces can be used in the evaluated configuration:

You can install Network Director in one of the following appliances:

- Juniper Networks JA2500 Junos Space Hardware Appliance—The JA2500 appliance is a dedicated hardware device that provides the computing power and specific requirements to run Network Director and the Network Director API as applications.

  The JA2500 appliance has a 2-U, rack-mountable chassis with dimensions 17.81 in. x 17.31 in. x 3.5 in. (45.2 cm x 44 cm x 8.89 cm). The JA2500 appliance ships with a single AC power supply module; an additional power supply module can be installed in the power supply slot in the rear panel of the appliance. The JA2500 appliance can also be powered on by using one or two DC power supply modules. The appliance has six 1-TB hard drives arranged in a RAID 10 configuration. Two externally accessible cooling fans provide the required airflow and cooling for the appliance.

For details about the JA2500 appliance and instructions for installation, see Juniper Networks JA2500 Junos Space Appliance.

- Junos Space Virtual Appliance—The Junos Space Virtual Appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain. A Junos Space Virtual Appliance includes the same software and provides all the functionality available in a Junos Space physical appliance. However, you must deploy the virtual appliance on the VMware ESX or ESXi server 6.5, which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional.

  For information about installing Junos Space appliances in a fabric configuration and installing Junos Space Virtual Appliance on a VMware ESX or ESXi server 6.5, see Junos Space Virtual Appliance.

Setting Up User and System Preferences

IN THIS SECTION

- Accessing the Preferences Page | 33
- Choosing Server Time or Local Time | 34
- Specifying Search Preferences | 34
- Enabling Import of Configuration Group Data from Ethernet Design | 34
- Specifying the Open Clos Server URL | 35
- Selecting the Approval Mode | 35
- Setting up Auto-resynchronization Preferences | 36
- Retaining Network Director Reports | 37
- Specifying Wireless Preferences | 37
- Changing Monitor Mode Settings | 37
- Changing Alarm Settings | 44
- Modifying Data Center Synchronization Interval Using the Virtualization Tab | 60

Depending on your privileges, the Preferences page displays either user settings or a combination of user settings and system settings. One or more of the following preference tabs appear when you open the Preferences page:

- User—All users can choose whether monitors and reports display the local time or the server time.
- Search—Network administrators can configure options for search indexing.
- Config & Deploy—Network administrators can:
  - choose to enable or disable import of configuration group data into Network Director.
  - specify the Auto Approval or Manual Approval mode for device configuration deployments.
- Monitoring—As a network administrator you can change the polling interval for data collection for Monitor mode monitors and enable or disable the internal processes used for data collection. You can also specify the IP address of the Data Learning Engine server, if installed, and the database record retention periods.
- Fault—As a network administrator you can enable or disable alarms. They can also set the retention period for alarms and the number of events per alarm.
- Report—Network administrators can specify the period of time for which Network Director reports are retained.
- Wireless—Network administrators can specify the Aruba Airwave application and RingMaster URLs.
- Topology—Network administrators can specify a retention period for the deleted links in Topology view.
- Virtualization—Network administrators can modify the synchronization time interval between Network Director and the cloud infrastructure.

This topic describes:

Accessing the Preferences Page

To open the Preferences page, click in the Network Director banner and select **Preferences** as shown in Figure 8 on page 33.

Figure 8: Accessing the Preferences Page

The Preferences page opens with User Preferences as the default tab.

Choosing Server Time or Local Time

All users can specify whether Network Director displays local time or the server's time in monitors and reports on the User Preferences tab. The default setting is to display local time. To change the setting to display the server's time:

1. In the Preferences page, select **Use Server Time** from the list.

2. Click **OK** to save your changes or click **Cancel** to close Preferences.

Specifying Search Preferences

Network Director indexes the device inventory data periodically to enable users to perform efficient searches. You can specify a time interval after which Network Director initiates the next indexing on the Search tab. You can also specify to stop indexing while devices are imported into Network Director. If you are running short of system memory, selecting this option helps save some memory and speed up the discovery and import of new devices. By default, this option is selected and the search index update interval is set to 900 seconds.

Enabling Import of Configuration Group Data from Ethernet Design

For Network Director to be able to import configuration group data.

To enable the import of configuration group data:

1. In the Preferences window, select the **Config & Deploy** tab.

2. Select the **Enable migration from Ethernet Design** check box to enable import of configuration group data. By default this check box is not selected.

3. Click **Save** to save and close the preferences.

   For detailed steps on importing configuration group data from Ethernet Design, see *Importing Configuration Data from Junos OS Configuration Groups*.

Specifying the Open Clos Server URL

Layer 3 Fabrics can expand your data center network to thousands of ports. Network Director uses Layer 3 protocols and Open Clos architecture to achieve this. Open Clos is typically installed on a separate system. You must specify the URL of the Open Clos system in Network Director before you can create and manage Layer 3 Fabrics.

To specify the URL for the Open Clos server:

1. Open the Config & Deploy tab in the Preferences window.
2. Enter the URL to the system that is running Open Clos.
3. Click **OK**.

Selecting the Approval Mode

Use the Config & Deploy tab of System Preferences to configure the approval mode:

1. Select the **Manual Approval** mode if you want an approver to review and approve the changes before they are deployed.

   By default, **Auto Approval** mode is selected. Use this mode if you want to deploy the configuration changes without a prior approval.
2. If you select the Manual Approval mode, add one or more approvers' e-mail addresses to notify the approvers every time a change request is submitted.
3. Specify the rollback limit, which is the number of change requests that can be rolled back.

   The default value is 50. You can roll back a maximum of 1000 change requests.
4. Specify the time after which a change request elapses after the time it was created.

   The minimum and maximum number of days that you can specify after which a change request elapses is 1 day and 365 days respectively. The change requests are highlighted in the following colors that indicate their overdue status.

   - Red color—Indicates that the change request is in overdue status.
   - Orange color—Indicates that the change request is due in less than 2 days.

- Green color—Indicates that the change request is not yet due.

5. Click **OK** to save the changes.

> **BEST PRACTICE:** Configuring the approval mode must be a one-time operation. Do not change the approval mode frequently.
>
> To change the approval mode from Auto Approval to Manual Approval, you must either deploy or discard the device configuration changes. You are unable to change the approval mode to Manual Approval, or from Manual Approval to Auto Approval if local changes are in pending deployment state. The message: **Do you want to retain the Change Request history?** is displayed when you change the approval mode. If you choose to retain the change request history, all the existing change requests are retained by the system. Hence, even if you switch to the Auto Approval mode, you can view the change requests that were created in Manual Approval mode.

> **NOTE:** While configuring the Manual Approval mode, you can specify any number of approvers. If you specify more than one approver while configuring the Manual Approval mode, after any approver accepts or rejects a proposed change, the change request is not listed for the other approvers and they cannot approve or reject the same change request.

Setting up Auto-resynchronization Preferences

If you enable auto-resynchronization in Network Director, any configuration changes made on the physical device, including out-of-band CLI commits and change-request updates, automatically trigger resychronization on the device.

To set up auto-resynchronization:

1. Select the **Config & Deploy** tab in the Preferences window.

2. Select the option **Purge unassigned system profiles after resynchronizing configuration**, which removes unassigned profiles generated by Network Director after resynchronization or deletion of a device.

> **NOTE:** While upgrading Network Director, the profiles that are in unassigned state are not removed even if you select this option.

3. Specify the time interval in **Auto Resync TriggerWait Interval(sec)**. Network Director waits for this time interval before triggering auto-resynchronization.

   The default time interval is 120 seconds.

4. Click **OK**.

Retaining Network Director Reports

By default, Network Director retains reports for 30 days. However, Network Administrators can change the retention period within the range 0 through 365 days. To change the setting, move the slider right or left on the Report tab of Preferences to the new setting. Click **OK** to save the setting.

Specifying Wireless Preferences

To manage Aruba wireless devices in your network, specify the URL to launch the Aruba's wireless management platform, the Aruba Airwave application.

Sites with Aruba Airwave application licenses can launch the Airwave application from within Network Director by supplying the Airwave application URL. For information about setting up preferences to launch the Aruba Airwave application, see *Linking to the Aruba Airwave Application*.

To manage Juniper wireless devices in your network, specify the URL to launch Juniper's wireless management platform, RingMaster.

Sites with RingMaster licenses can launch the RingMaster application from within Network Director by supplying the RingMaster URL. After typing the URL on the Wireless tab of Preferences, you can click **Launch RingMaster** in Build mode to load RingMaster into the main page. To enable launching RingMaster from within Network Director, simply type in the URL and click **OK** to save the setting.

Changing Monitor Mode Settings

IN THIS SECTION

- Disabling Data Collection for Monitors | 38
- Changing the Polling Interval | 40

Enabling and Disabling Collection for Managed Devices | 41
Specifying Database History Retention | 42
Specifying the Data Learning Engine (DLE) Settings | 42

The Monitoring tab of Preferences has three tabs under it. These are:

- Monitoring Settings—Enables you to change the default polling interval for data collection for Monitor mode monitors. You can also disable or reenable the internal processes used for data collection on this sub-tab.
- Client Session History—Enables you to set the retention period for history records and the frequency that these records are checked for deletion.
- Data Learning Engine Settings—Enables you to specify the IP address of the Data Learning Engine (DLE) server or servers, which is a component of Cloud Analytics Engine that supports the flow path analysis and high-frequency statistics features in Network Director.
- Device Settings—Allows you to enable or disable data collection for one or more devices.

This section describes:

Disabling Data Collection for Monitors

Network Director internally gathers data for monitors by using a set of data collection processes. You can disable these data collectors if they do not pertain to your installation. For example, if you do not use Virtual Chassis, you can disable the data collection processes used for Virtual Chassis.

The data collection processes are divided into the following categories:

- Client
- Equipment
- FM
- RF
- Traffic
- Virtual

One data collector can be used by multiple monitors. Likewise, some monitors can be supported by multiple data collectors. These data collectors are enabled by default. To ensure proper data collection, if you enable the equipment data collectors, you must also enable the traffic collectors..

To disable or reenable a data collector:

1. Determine which monitors are used by the data collectors. Use Table 6 on page 39 to determine the relationship between the data collectors and the monitors.

Table 6: Monitor Mapping for Data Collectors

Monitor	Data Collector	Category
802.11 Packet Error	RFMonitorRadioStatsCollector	RF
AP Interference Source	RFMonitorIntSourcesCollector	RF
AP Status	EquipmentMonitorAPCollector	Equipment
Current Sessions	Client Monitor Collector and SessionCountCollector	Client
Error Trend	PortTrafficMonitorCollector	Traffic
Logical Interfaces	EquipmentMonitorDeviceStatusCollector	Equipment
Find End Point	EquipmentMonitorEndPointCollector	Equipment
Percentage of Packets Retransmitted	RFMonitorRadioStatsCollector	RF
Port Status (physical)	EquipmentMonitorDeviceStatusCollector	Equipment
Radio Status	EquipmentMonitorAPCollector	Equipment
RF Neighborhood	RFMonitorRadioNeighborCollector	RF
RF Throughput or Packet Retransmitted	RFMonitorRadioStatsCollector	RF
Resource Utilization	EquipmentMonitorDeviceStatusCollector	Equipment
Session Trend	ClientMonitorCollector and SessionCountCollector	Client
Switch Status	EquipmentMonitorDeviceStatusCollector	Equipment
Traffic Trend	PortTrafficMonitorCollector	Traffic

Table 6: Monitor Mapping for Data Collectors *(continued)*

Monitor	Data Collector	Category
Top Sessions by MAC Address	ClientMonitorCollector	Client
Top Users	ClientMonitorCollector	Client
Unicast vs Broadcast/Multicast	PortTrafficMonitorCollector	Traffic
Unicast vs Broadcast/Multicast Trend	PortTrafficMonitorCollector	Traffic
Virtual Chassis Topology	EquipmentMonitorVCStatsCollector and EquipmentMonitorDeviceStatusCollector	Equipment
Virtual Chassis Protocol	EquipmentMonitorVCStatsCollector and EquipmentMonitorDeviceStatusCollector	Equipment
Virtual Chassis Statistics	EquipmentMonitorVCStatsCollector and EEquipmentMonitorDeviceStatusCollector	Equipment

2. Clear the check box to disable the collector or select to enable the collector.

3. Click **Save** and **Close** to save the configuration and to close the window.

Changing the Polling Interval

The frequency at which data is collected is determined by the polling interval. Table 7 on page 40 shows the default polling intervals used by each data collector.

Table 7: Default Polling Intervals

Collector	Polling Interval
ClientMonitorCollector	10 minutes
SessionCountCollector	10 minutes
EquipmentMonitorVCStatsCollector	30 minutes
EquipmentMonitorAPCollector	10 minutes
EquipmentMonitorEndPointCollector	1440 minutes

Table 7: Default Polling Intervals *(continued)*

Collector	Polling Interval
EquipmentMonitorDeviceStatusCollector	10 minutes
FMAlarmCountCollector	10 minutes
RFMonitorIntSourcesCollector	15 minutes
RFMonitorRadioNeighborCollector	15 minutes
RFMonitorRadioStatsCollector	10 minutes
PortTrafficMonitorCollector	10 minutes
VirtualHostPMCollector	10 minutes
VirtualNICStatsCollector	10 minutes
VirtualMachineStatsCollector	10 minutes
VirtualMachineWeeklyStatsCollector	30 minutes

To change the polling interval:

1. Select the polling interval for a data collector in the Monitor Settings table.

2. Type the new interval level in whole minutes. For example, do not specify 1.5 minutes. Recommended intervals are 5, 10, or 20 minutes.

3. Click **OK** and then **Yes** to verify the change to the configuration.

Enabling and Disabling Collection for Managed Devices

By default all the devices that are discovered and managed by Network Director are enabled for data collection. You can disable or re-enable data collectors across all categories for devices that are managed by Network Director from this tab.

To enable or disable data collectors for devices

1. Open the **Device Settings** sub-tab in the Monitor tab.

   All the devices that are managed by Network Director is displayed in the Device Settings section. The last column of the device table indicates the status of data collection as Enabled or Disabled.

2. Select the devices for which you want to enable or disable data collection and do one of the following:
   - Click **Enable** to enable data collection for the selected devices.
   - Click **Disable** to disable data collection for the selected devices.

Specifying Database History Retention

To keep the database manageable, the system periodically checks the age of the records and retires those that have past an expiration date. By default, Network Director ages database records off at 90 days and runs a database cleanup every 6 hours.

Use the Client Session History sub-tab to change the default values:

1. Select from the lists new values.
   - Age of history records (in days) from 1 to 365 days.
   - Cleanup job frequency (in hours) from 1 through 24 hours.
2. Click **OK** to save the changes.

Specifying the Data Learning Engine (DLE) Settings

The Data Learning Engine (DLE) is the component of Cloud Analytics Engine that enables Network Director to collect and analyze high-frequency statistics data from devices and to perform flow path analysis. For Network Director to use Cloud Analytics Engine, you must specify on what server or servers the Data Learning Engine (DLE) is running.

Each DLE supports up to a specific number of Compute Agents (CAs) running on network devices. If you have more CAs in a network than a single DLE can support, you might require multiple DLEs.

Use the Data Learning Engine Settings sub-tab under the Monitoring tab to specify which Data Learning Engine (DLE) server or servers Network Director uses. You can also change the default ports used by the DLE.

To configure DLE in Network Director:

1. Log in to Network Director.

2. Select **Preferences** from the list next to the **System** button in the Network Director banner.

   The Preferences page is displayed.

3. Select the **Monitoring** tab and then select **Data Learning Engine Settings**.

4. Enable DLE only with HTTPS TLSv1.2 configured with SHA256 RSA 2048 signature. In the **DLE IP Address** field, enter the IP address of the DLE server.

   NOTE: Before you configure DLE in Network Director, make sure that there are no errors in the monitor.log file. The log file is stored in the **/var/log/jboss/server/server1** directory.

5. If you want to change the ports used by the DLE, click **View/Edit DLE Ports** to edit the ports and then click **OK**.

   NOTE: If you change the default DLE ports (8282, 8081, and 50006), you must ensure that the new ports are open between DLE and Junos Space Network Management Platform or Network Director.
   You can use the **netstat -anp | grep *port-number*** command to verify that the new ports are open (in listening mode) between DLE and Junos Space Network Management Platform or Network Director.

   Table 8 on page 43 describes the default DLE ports.

   Table 8: Default DLE Port Descriptions

Port	Description
Flow Analysis API Port	Used by the flow path analysis feature and network traffic analysis feature to communicate with the DLE. Default value is 8282.
HFS API Port	Used by the high-frequency statistics feature to communicate with the DLE. Default value is 8081.
HFS Control Channel Port	Used by the high-frequency statistic feature for communication about threshold-related events with the DLE. Default value is 50006.

6. Click **OK** to save the DLE settings.

   The message **Preferences saved successfully** is displayed.

> **NOTE:** After you configure the DLE settings, check whether the DLE connection state is **UP** in the DLE settings page.

7. Click **Add Another** to add a new DLE server.

Changing Alarm Settings

IN THIS SECTION

- Configuring Global Alarm Notifications | 44
- Retaining Alarm History | 45
- Specifying Event History | 45
- Enabling Alarms | 45
- Changing the Severity of Individual Alarms | 59
- Configuring Threshold Alarms | 59
- Configuring Individual Alarm Notifications | 59

Use the Fault tab to enable individual alarms, set the retention period for alarms, configure alarm notifications, configure threshold alarms, and to specify the number of events to keep for each alarm. The Fault tab has multiple sections, which you can expand and collapse by clicking the arrow next to the section title:

- Global Settings, for configuring Faults settings such as global alarm notifications and alarm data retention.
- Individual Alarms and Threshold Settings, for configuring settings for individual alarms and threshold alarms.

This section describes the following tasks that you can perform by using the Fault tab:

Configuring Global Alarm Notifications

You can configure global e-mail notifications to be sent when any alarm with notifications enabled is generated. To configure global e-mail notifications, enter the e-mail addresses to receive global alarm notifications in the Alarm Notifications Destinations field in the Global Settings section. Separate addresses

with a comma (,). For information about enabling notification for an alarm, see "Configuring Individual Alarm Notifications" on page 59.

Retaining Alarm History

Use the **No. of days to keep Alarm** field in the Global Settings section to specify the number of days to keep alarm history. The default retention time is 120 days; but you can specify a period of 7 through 1000 days. Specifying a longer retention time consumes more database resources. To change the alarm retention duration, type a new value and click **OK** and **Yes** to confirm the change.

Specifying Event History

Use the **Events/Alarm** field in the Global Settings section to specify the number of event entries that are kept in the alarm history. The default setting for events is 20. To change the setting, type a new value and click **OK** and **Yes** to confirm the change.

Enabling Alarms

Ensure all devices are configured to send traps to Network Director. This task is performed for the devices in Deploy mode through Set SNMP Trap Configuration.

Use the Individual Alarms and Threshold Settings section to disable and re-enable individual alarms or all alarms. Alarms appear on both tabs in the section: Alarm Settings and Threshold Settings. Fault alarms are preconfigured and initially enabled. To enable or disable alarms:

1. (Optional) Sort the alarms. By default, the list of alarms is sorted alphabetically within each category. You can also sort by description or alarm severity within a category by clicking a column heading.

2. Review the alarms and either select the check box in the heading to select all of the alarms or select the check box for the individual alarms you want to enable. For a full description of each of the alarms, see Table 9 on page 45.

3. Click **OK** and **Yes** to confirm the alarm change.

Table 9: Alarm Descriptions

Alarm Name	Description	Device Type
AP and Radio (AP/Radio)		

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
AP License Limit Exceeded	Generated when the number of wireless LAN access points (WLAs) exceed the number of licenses configured on a wireless switch. The trap occurs when a wireless switch receives a packet from an inactive access point. The switch is unable to attach the access point without exceeding the maximum (licensed) number of active access points.	Wireless LAN controller
AP Manager Changed Alarm	Generated when the access point's secondary link becomes the primary link.	Wireless LAN controller
AP Status Alarm	Generated when an access point changes state.	Wireless LAN controller
AP Tunnel Limit Exceeded	Generated when the number of tunnels on an access point exceeds the maximum number supported. This alarm is generated by the access point's Primary Access Manager (PAM) when the access point rejects a tunnel creation request because it has already created the maximum number of tunnels it can support.	Wireless LAN controller
M2U Conversion	Generated when multicast to unicast conversion is enabled on the access point, but cannot be performed.	Wireless LAN controllers
Radio Channel Changed	Generated when auto-tune changes a radio's channel.	Wireless LAN controller
Radio power changed	Generated when auto-tune changes a radio's power level.	Wireless LAN controller
Radio Status Alarm	Generated when a radio changes state. It also contains aggregate information about the access point in operational state, its security level and service availability.	Wireless LAN controller

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
WLC Tunnel Limit Exceeded	Generated when the wireless switch rejects a tunnel creation request because it has reached the maximum number of tunnels supported. When the trap event trpzWsTunnelLimitType equals the platform-tunnel-limit, the wireless switch has reached the maximum tunnel capacity. The actual tunnel limit varies by platform. When the trap trpzWsTunnelLimitType equals ap-ws-tunnel-limit, the wireless switch has reached the access point-to-switch tunnel's limit. The value of that limit depends on the current situation of the wireless switch (mobility domain, network domain, network and resiliency status).	Wireless LAN controller
BFD		
BfdSessionDetectionTimeAlarm	Generated when the threshold value for detection time is set and the BFD session detection-time adapts to a value greater than the threshold.	EX Series Switch
BfdSessionTxAlarm	Generated when the threshold value for transmit interval (in microseconds) is exceeded.	EX Series Switch
BGP		
BgpM2BackwardTransitionAlarm	Generated when the BGP FSM moves from a higher-numbered state to a lower-numbered state.	EX Series Switch
BgpM2EstablishedAlarm	Generated when the BGP Finite State Machine (FSM) enters the ESTABLISHED state.	EX Series Switch
Chassis		
FanFailureAlarm	Generated when the specified cooling fan or impeller has failed (is not spinning).	EX Series Switch
FEBSwitchoverAlarm	Generated when the Forwarding Engine Board (FEB) has switched over.	EX Series Switch

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
FRUCheckAlarm	Generated when the device has detected that a field-replaceable unit (FRU) has some operational errors and has gone into check state.	EX Series Switch
FRUFailedAlarm	Generated when a FRU has failed.	EX Series Switch
FRUInsertionAlarm	Generated when the system detects that the specified FRU is inserted into the chassis.	EX Series Switch
FRUOfflineAlarm	Generated when the specified FRU goes offline.	EX Series Switch
FRUOnlineAlarm	Generated when the specified FRU goes online.	EX Series Switch
FRUPowerOffAlarm	Generated when the specified FRU is powered off.	EX Series Switch
FRUPowerOnAlarm	Generated when the specified FRU is powered on.	EX Series Switch
FRURemovalAlarm	Generated when the system detects that the specified FRU was removed from the chassis.	EX Series Switch
HardDiskFailedAlarm	Generated when the hard disk for the specified routing engine has failed.	EX Series Switch
HardDiskMissingAlarm	Generated when the hard disk in the specified routing engine is missing from the boot device list.	EX Series Switch
PowerSupplyFailureAlarm	Generated when the specified power supply has failed (bad DC output).	EX Series Switch
RedundancySwitchOverAlarm	Generated when a graceful Routing Engine switchover (GRES) occurs on a switch with dual Routing Engines or on a Virtual Chassis.	EX Series Switch
TemperatureAlarm	Generated when the device has over heated.	EX Series Switch

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Client and User Session (ClientAndUserSession)		
Client Association Failure	Generated when a client is unable to associate with an access point.	Wireless LAN controller
Client Authentication Failure	Generated when a client is unable to authenticate.	Wireless LAN controller
Client Authorization Failure	Generated when a client fails authorization.	Wireless LAN controller
Client Authorization Succeeded	Generated when a client authorizes.	Wireless LAN controller
Client Cleared	Generated when a client session is cleared.	Wireless LAN controller
Client Connectivity	Generated when a client session connects.	Wireless LAN controller
Client DeAssociated	Generated when a client de-association occurs.	Wireless LAN controller
Client DeAuthenticated	Generated when a client de-authenticates.	Wireless LAN controller
Client Disconnected	Generated when a client session disconnects administratively.	Wireless LAN controller
Client dot1x Failure	Generated when a client fails 802.1x.	Wireless LAN controller
Client Dynamic Authorization Changed	Generated when the authorization attributes for a user are dynamically changed by a authorized dynamic authorization client.	Wireless LAN controller
Client IP Address Changed	Generated when a client's IP address changes, normally when the client first connects to the network.	Wireless LAN controller

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Client Roamed	Generated when a client roams from one location to another.	Wireless LAN controller
Dynamic Authorization Client Alarm	Generated when the authorization attributes for a user are dynamically changed by an authorized dynamic authorization client.	Wireless LAN controller
Cluster/Modo		
Cluster Sync Failure	Generated when the cluster configuration failed to apply.	Wireless LAN controller
Mobility Domain Failback	Generated when the mobility domain fails back to the primary seed.	Wireless LAN controller
Mobility Domain Failover	Generated when the mobility domain fails back to the secondary seed.	Wireless LAN controller
Mobility Domain Join	Generated when a member joins the mobility domain.	Wireless LAN controller
Mobility Domain Resiliency Status	Generated when a mobility domain seed changes resilient capacity.	Wireless LAN controller
Mobility Domain Timeout	Generated when a mobility domain member times out.	Wireless LAN controller
Configuration (Configuration)		
CmCfgChangeAlarm	Generated when the jnxCMCfgChgEventTable records a configuration management event.	EX Series Switch and wireless LAN controller
CMRescueChangeAlarm	Generated when a change is made to the rescue configuration.	EX Series Switch and wireless LAN controller
Core and controllers (Controllers)		

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Device alarm	Generated when the device status changes (up to down or down to up).	EX Series Switch and wireless LAN controller
CoS		
CoSAlmostOutOfDedicatedQueuesAlarm	Generated when only 10% of CoS queues are available.	EX Series Switch
CoSOutOfDedicatedQueuesAlarm	Generated when there are no more available dedicated CoS queues.	EX Series Switch
DHCP		
JdhcpLocalServerDupClientAlarm	Generated when a DHCP client is detected changing interfaces.	EX Series Switch
JdhcpLocalServerIfLimitExceededAlarm	Generated when the client limit is reached on an interface.	EX Series Switch
Jdhcpv6LocalServerLimitExceededAlarm	Generated when the client limit is reached on an interface for DHCPv6.	EX Series Switch
DOM		
DomAlertSetAlarm	Generated when an interface detects Digital Optical Monitor (DOM) alarm conditions.	EX Series Switch
Flow Collection (FlowCollection)		
CollFlowOverloadAlarm	Generated when a collector PIC detects a hard or soft flow overload.	EX Series Switch
CollFtpSwitchOverAlarm	Generated when an FTP server switchover occurs.	EX Series Switch
CollMemoryUnavailableAlarm	Generated when a PIC is out of memory or the memory is unavailable.	EX Series Switch
CollUnavailableDestAlarm	Generated when a file transfer destination is unavailable.	EX Series Switch

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
CollUnsuccessfulTransferAlarm	Generated when a collector file is unable to transfer because the destination is unavailable.	EX Series Switch
General		
Authentication Failure Alarm	Generated when a protocol message is received that is not properly authenticated.	EX Series Switch and wireless LAN controller
Cold Start Alarm	Generated when a device is re-initializing and its configuration might have changed.	EX Series Switch and wireless LAN controller
Link Down Alarm	Generated when a link is down. The trap is generated when the ifOperStatus object for a communication link is about to enter the down state from another state other than notPresent. This other state is indicated by the included value of ifOperStatus.	EX Series Switch and wireless LAN controller
Link Up Alarm	Generated when a link comes up that was previously in the down state. The trap is generated when the ifOperStatus object for a communication link left the down state and transitioned into another state other than notPresent state. This other state is indicated by the included value of ifOperStatus.	EX Series Switch and wireless LAN controller
Warm Start Alarm	Generated when a device is re-initializing and its configuration has not changed.	EX Series Switch and wireless LAN controller
Generic (GenericEvent)		
GenericEventTrapAlarm	Generated by an Op script or event policies. This notification can include one or more attribute-value pairs. The pairs are identified by the jnxEventAvAttribute and jnxEventAvValue objects.	EX Series Switch
L2ALD		

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
L2aldGlobalMacLimitAlarm	Generated when the MAC limit is reached for the entire system. This trap is sent only once, when the limit is reached.	EX Series Switch
L2aldInterfaceMacLimitAlarm	Generated when the given interface reaches the MAC limit (jnxl2aldInterfaceMacLimit).	EX Series Switch
L2aldRoutingInstMacLimitAlarm	Generated when the MAC limit is reached for a given routing instance (jnxl2aldRoutingInst).	EX Series Switch
L2CP		
LacpTimeOutAlarm	Generated when LACP has timed out.	EX Series Switch
PortBpduErrorStatusChangeTrapAlarm	Generated when the port's BPDU error state (no-error or detected) changes.	EX Series Switch
PortLoopProtectStateChangeTrapAlarm	Generated when the port's loop-protect state (no-error or loop-prevented) changes.	EX Series Switch
PortRootProtectStateChangeTrapAlarm	Generated when the port's root-protect state (no-error or root-prevented) changes.	EX Series Switch
MAC Forwarding Database (MACFDB)		
MacChangedNotificationAlarm	Generated when MAC addresses of the monitored devices are learned or removed from the forwarding database (FDB).	EX Series Switch and wireless LAN controller
Misc.		
Counter Measures Alarm	Generated when counter measures are started against a rogue device.	Wireless LAN controller
Device Configuration Saved	Generated when the running configuration of the switch is written to the configuration file.	Wireless LAN controller
Multimedia Call Failure	Generated when a multimedia call fails.	Wireless LAN controller
PoE (Power over Ethernet)		

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
PoE Port ON-OFF Alarm	Generated when the PoE power is turned on or off.	EX Series Switch
PoE Power Usage High	Generated when Power over Ethernet (PoE) used is below or above the defined threshold.	EX Series Switch
Passive Monitoring (PassiveMonitoring)		
PMonOverloadSetAlarm	Generated when an overload condition is detected on a Passive Monitoring Interface.	EX Series Switch
Ping		
PingEgressJitterThresholdExceededAlarm	Generated when egress time jitter (jnxPingMaxEgressUs minus jnxPingResultsMinEgressUs) exceeds the configured threshold (jnxPingCtlEgressJitterThreshold) causing the egressJitterThreshold bit to be set.	EX Series Switch and wireless LAN controller
PingEgressStdDevThresholdExceededAlarm	Generated when the standard deviation of the egress time (jnxPingResultsStddevEgressUs) exceeds the configured threshold (jnxPingCtlEgressTimeThreshold) and causes the egress bit to be set.	EX Series Switch and wireless LAN controller
PingEgressThresholdExceededAlarm	Generated when the egress time (jnxPingResultsStdevEgressUs) exceeds the configured threshold (jnxPingCtlEgressTimeThreshold) and the egress threshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingIngressJitterThresholdExceededAlarm	Generated when ingress time jitter (jnxPingResultsMaxIngressUs minus jnxPingResultsMinIngressUs) exceeds the configured threshold (jnxPingCtlIngressJitterThreshold) and the ingressJitterThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
PingIngressStddevThresholdExceededAlarm	Generated when the standard deviation of the ingress time (jnxPingResultsStdDevIngressUs) exceeds the configured threshold (jnxPingCtlIngressStddevThreshold) and the ingress StdDevThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingIngressThresholdExceededAlarm	Generated when the ingress time jitter (jnxPingResultsIngressUs) exceeds the configured threshold (jnxPingCtlIngressTimeThreshold) and the ingress threshold bit (jnxPingIngressThresholdExceeded) is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingRttJitterThresholdExceededAlarm	Generated when the round trip time jitter (jnxPingResultsMaxRttUs minus jnxPingResultsMinRttUs) exceeds the configured threshold (jnxPingCtlRttJitterThreshold) and the rttJitterThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingRttStdDevThresholdExceededAlarm	Generated when the standard deviation of the round trip time (jnxPingResultsStdDevRttUs) exceeds the configured threshold (jnxPingCtlRTTStdDev) and the rttStdDevThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
PingRttThresholdExceededAlarm	Generated when the round trip time (jnxPingCtlRttThreshold) exceeds the configured threshold (jnxPingCtlRttThreshold) and the rttThreshold bit is set in jnxPingCtlTrapGeneration.	EX Series Switch and wireless LAN controller
RF Detect (RFDetect)		
Adhoc user detected	Generated when RF detection sweep finds an ad hoc user or if a previously found ad hoc user disappears.	Wireless LAN controller

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Client Blocklisted	Generated when an association, re-association, or de-association request is detected from a blocklisted transmitter.	Wireless LAN controller
DoS Attack Detected	Generated when RF detection finds a denial-of-service (DoS) attack occurring.	Wireless LAN controller
DoS Port Detected	Generated when RF detection finds a denial of service (DoS) attack occurring. This trap collects port and access point information instead of information about the listener.	Wireless LAN controller
RF Interference Detected	Generated when a new noise source appears. A given combination of noise source ID, listener, and channel triggers this trap. It is normally not triggered more than once every 15 minutes.	Wireless LAN controller
RF Detect Classification Changed	Generated when the RF detection classification rules change.	Wireless LAN controller
Rogue Device Detected	Generated when RF detection finds a rogue device.	Wireless LAN controller
Rogue Wired WLA Client Detected	Generated when a client is detected that connected through a rogue access point that is attached to a wired port.	Wireless LAN controller
Rogue WLA Client Detected	Generated when RF detection finds a suspect device.	Wireless LAN controller
Rogue WLA Interference Detected	Generated when RF detection finds an interfering rogue access point.	Wireless LAN controller
Spoofed MAC Detected	Generated when RF detection finds an access point using the MAC of the listener.	Wireless LAN controller
Spoofed SSID Detected	Generated when RF detection finds an access point using the SSID of the listener, and the access point is not in the mobility domain.	Wireless LAN controller

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Suspected Device Detected	Generated when RF detection finds a suspect device.	Wireless LAN controller
Unauthorized AP Detected	Generated when RF detection discovers an unauthorized access point being used.	Wireless LAN controller
Unauthorized OUI Detected	Generated when RF detection finds an unauthorized OUI being used.	Wireless LAN controller
Unauthorized SSID Detected	Generated when RF detection finds an unauthorized SSID being used.	Wireless LAN controller
RMon		
RmonAlarmGetFailureAlarm	Generated when a GET request for an alarm variable returns an error. The specific error is identified by a varbind in jnxRmonAlarmGetFailReason.	EX Series Switch
SONET		
SonetAlarmSetAlarm	Generated when there is a notification of a recently set SONET or SDH alarm on an interface.	EX Series Switch
SONET APS (SONETAPS)		
APSEventChannelMismatchAlarm	Generated when the value of an instance of apsStatusChannelMismatches increments.	EX Series Switch
APSEventFEPLFAlarm	Generated when the value of an instance of apsEventFEPLFs increments.	EX Series Switch
APSEventModeMismatchAlarm	Generated when the value of an instance of apsEventModeMismatch increments.	EX Series Switch
APSEventPSBFAlarm	Generated when the value of an instance of apsStatusPSBFs increments.	EX Series Switch
APSEventSwitchoverAlarm	Generated when the value of an instance of apChanStatusSwitchover increments.	EX Series Switch

Table 9: Alarm Descriptions *(continued)*

Alarm Name	Description	Device Type
Virtual Chassis (VirtualChassis)		
VccpMemberAlarm	Generated when a member has completed transition from the down state to another state.	EX Series Switch
VccpPortAlarm	Generated when one of the member's communication links has completed transition from the down state to another state.	EX Series Switch
VNetwork		
HostConnectivityLostAlarm	Generated when all the uplink ports of a virtual switch residing in a host loses network connectivity.	Host
HostNetworkRedundancyLostAlarm	Generated when some uplink ports of a virtual switch residing in a host loses network connectivity. It indicates that there are one or more ports that still has network connectivity.	Host
VNetworkConnectivityLostAlarm	Generated when Network Director loses network connectivity with the vCenter server.	Virtual Network

Changing the Severity of Individual Alarms

You can change the severity of the alarms to match your corporate procedures and guidelines. For example, at your company a DoS attack might be considered a critical alarm, while Network Director has a default severity for DoS attacks as a major alarm. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To change the severity of an alarm:

1. Select the current severity in the **Severity** column. A list of the severity levels appear.
2. Select the new severity level for the alarm.
3. Click **OK** and **Yes** to confirm the change to the severity setting.

   To configure alarm notifications, see "Configuring Individual Alarm Notifications" on page 59.

Configuring Threshold Alarms

Threshold alarms are alarms that are generated when a monitored value crosses the configured threshold. They provide enhanced visibility into potential issues on the network. You configure and manage threshold alarms the same way as other alarms. You also have the option of setting the threshold level of individual threshold alarms.

To edit the threshold of threshlod alarms:

1. Select the **Threshold Settings** tab in the Individual Alarms and Threshold settings section of the Fault tab.
2. Click **Edit Settings** in the Threshold Settings column of the alarm threshold you want to edit.
3. Set the threshold in the window that opens.
4. Click **Save** to save the new threshold.

   To configure alarm notifications, see "Configuring Individual Alarm Notifications" on page 59.

Configuring Individual Alarm Notifications

You can configure e-mail notifications to be sent when an individual alarm is generated. When you enable notification for an alarm, the notifications are sent to the e-mail addresses configured for the alarm and the addresses configured for global alarm notifications. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To configure e-mail notification for an alarm name:

1. Select the check box in the alarm's Notification column.

   If you later want to disable notification for the alarm, clear the check box.

2. Click **Edit Notification** in the Notification column. The Alarm Notification Details window opens.

3. Type one or more e-mail addresses in the **Notification Email Addresses** box. Separate addresses with a comma (,).

   You can later edit the addresses to send notifications to different addresses.

4. (Optional) Type a comment in the Comments box. This comment is included in the e-mail notification message.

5. Click **Save**.

Modifying Data Center Synchronization Interval Using the Virtualization Tab

You can configure and manage data centers by using the Data Center View in Network Director. Network Director synchronizes data from the cloud infrastructure that is part of your data center every 24 hours. However, depending on the size of your data center network, you can modify this interval from the Virtualization tab in the Preferences page. Modify the interval by changing the **Periodic Cloud Infrastructure Synchronization Interval (hours)** field.

For data centers that use OpenStack as the cloud infrastructure provider, Network Director displays the links between hypervisors and switches only in the Data Center View. If you want to view the link details using the View Virtual Network Connectivity task, then you must select the **Synchronize links from Topology to Virtualization application for OpenStack** check box.

> **NOTE:** Selecting the **Synchronize links from Topology to Virtualization application for OpenStack** check box might impact the performance of Network Director, while the synchronization is in process.

2

CHAPTER

Understanding Roles and Authentication Methods

Understanding Roles and Services for Network Director in FIPS Mode | **62**

Understanding Password Specifications and Guidelines for Network Director in Junos Space in FIPS Mode | **63**

Understanding Roles and Services for Network Director in FIPS Mode

Network Director uses the user administration features of the Junos Space platform on which it runs. Use Junos Space for tasks such as adding, deleting, and editing user accounts and roles, and changing user passwords. Refer to the Junos Space documentation for information about user administration.

When Network Director is installed, some additional user administration options are available in Junos Space, which are specific to Network Director:

- In addition to the Super Administrator role, the following predefined roles are available for Network Director users:

  Network Director - Admin—Has access to all the Network Director tasks. This role is the system administrator role and has full privileges.

  Network Director - Engineer—Has access to either all the device management tasks or only those device management sub-tasks to which the Engineer role is mapped. These users can also view the device monitoring and fault management tasks.

  Network Director - Monitor—Has access to monitor the network status and performance or view the faults to determine the health of your network and take appropriate action.

  Network Director - Configuration Approver—Has access to provide additional privileges to approve the configuration changes in addition to all the tasks that a Config Admin can perform.

  Network Director - Image Admin—Has access to all the image management tasks.

  Network Director - Config Admin—Has access to create, edit, delete, assign, deploy profiles, and manage fabrics (VCF, QFabric, and IP Fabric).

  Network Director - Cloud Admin—Has access to create data center and perform other data center related tasks.

- You can create custom roles to grant users different access rights to the Network Director modes, group, dashboard widgets, and tasks. Users can access only those portions of the navigation hierarchy to which they are explicitly granted access through access privileges.

If you try to log in to Network Director using an account that does not have access rights to any Network Director modes, you will be redirected to Junos Space instead.

Access to Network Director system preferences is controlled by user access rights.

Understanding Password Specifications and Guidelines for Network Director in Junos Space in FIPS Mode

Ensure that the device is in FIPS mode before you configure the Super Administrator or any users. All passwords established for users by the Super Administrator must conform to the following Junos Space in FIPS mode requirements. Attempts to configure passwords that do not conform to the following specifications result in an error.

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
  - Uppercase letters
  - Lowercase letters
  - Digits
  - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size—for example, 20 characters for SHA-1 authentication.

Guidelines for strong passwords. Strong, reusable passwords can be based on letters from a favorite phrase or word and then concatenated with other unrelated words, along with added digits. In general, a strong password is:

- Easy to remember so that users are not tempted to write it down.
- Made up of mixed alphanumeric characters and punctuation. For FIPS compliance include at least one change of case, one or more digits, and one or more punctuation marks.
- Changed periodically.
- Not divulged to anyone.

Characteristics of weak passwords. Do not use the following weak passwords:

- Words that might be found in or exist as a permuted form in a system files such as **/etc/passwd**.
- The hostname of the system (always a first guess).
- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.

- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**root**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

3

CHAPTER

Deploying Network Director

Installing Network Director | **66**

Installing Hot Patch | **71**

Logging In to Network Director | **71**

Installing Network Director

IN THIS SECTION

- Installing Network Director From Junos Space Store | 66
- Installing Network Director by Manually Downloading the Network Director Application Image | 67
- Discovering Devices | 69

Before you begin:

- Configure a Junos Space Appliance or a Junos Space Virutal Appliance as a Junos Space node or as a specialized node used for fault monitoring and performance monitoring (FMPM). For more information, see Configuring a Junos Space Appliance as a Junos Space Node for configuring a Junos Space Appliance or see Configuring a Junos Space Virtual Appliance as a Junos Space Node.
- Uninstall Connectivity Services Director or Edge Services Director before you install Network Director on your system. Network Director cannot be installed on a system that has Connectivity Services Director or Edge Services Director already installed. For steps to uninstall a Junos Space Application, see Uninstalling a Junos Space Application.

You can install Network Director on Junos Space Network Management Platform by using one of the following methods:

Installing Network Director From Junos Space Store

Junos Space Platform provides Junos Space store from where you can download and install or upgrade Network Director in a single operation. On the Junos Space store pagPe, you can view the versions of Network Director that are compatible with the currently installed version of Junos Space Platform.

> **NOTE:** Before you install or upgrade Network Director by using Junos Space store, you must configure the credentials to access Junos Space Store. For information see, *Configuring and Managing Junos Space Store*.

To install Network Director from Junos Space Store:

1. Click **Administration > Applications > Junos Space Store**.

   The Junos Space Store opens. Junos Space Store lists all the applications that can be installed on the Junos Space Platform.

2. Click **Network Director**.

   The right-side of the page lists the Network Director versions that can be installed on Junos Space Platform.

3. (Optional) Select the **Show only compatible version** check box to list only the FIPS compatible versions of Network Director that can be installed on the current installed version of Junos Space Platform.

4. Click **Next** to install Network Director.

   The end user license agreement page appears.

5. Click **Accept and install** to install Network Director.

   The Network Director installation job status appears. The status indicates each step that is completed while Network Director is getting installed.

   Once installed successfully, Network Director is listed on the Applications page (**Administration > Applications**).

Installing Network Director by Manually Downloading the Network Director Application Image

Download the Junos Space Network Director Release 3.6 software image to the hard disk or to an SCP server. The SCP server where you download the Network Director image should be a Linux server. You can download the Network Director Software image from the Network Director Download Software page.

To install Junos Space Network Director:

1. Log in to Junos Space.

2. Click the add symbol (+) adjacent to the Administration and click **Applications**.

   The Administration > Applications page opens.

3. Click add symbol (+) symbol to add the Network Director application.

   The Add Application page opens.

4. You can upload the Network Director release image file by using HTTP or by using SCP:

   To upload the image file using HTTP:

   a. Click **Upload via HTTP**.

      The Upload Software via HTTP page opens.

   b. Click **Browse** to select the Network Director image file. You can either navigate to the local directory and select the Network Director software image, or copy and paste the download URL in the **Software File** if the image is not already downloaded to the local directory.

      Your browser opens a dialog box to browse the Network Director image file.

   c. Click **Open** to download the image file.

   d. Click **Upload** to upload the image file.

      A notification about the progress in the upload is displayed.

   To upload the image file using SCP if you have a Linux server:

   a. Click **Upload via SCP**.

      The Upload Software via SCP page opens.

      Enter the following secure copy credentials to upload the image from a remote server to Junos Space.

      - Enter the user name of the remote server.
      - Enter the password of the remote server and reenter the password in the Confirm Password field.
      - Enter the host IP address of the remote server.
      - Enter the path of the remote server to which you have copied the Network Director image file.

   b. Click **Upload** to load the Network Director image file into Junos Space.

      The Upload Application Job Information dialog opens.

5. Click **OK** to skip viewing the job results and to take you back to the Administration > Applications > Add Application page..

6. Select Network Director and click **Install**.

7. Click **OK** in the Application Configuration window dialog box.

You can check the Job Status page to view the progress of the installation job. Once the installation completes, Network Director appears on the Applications page. The Network Director application also appears in the Application Chooser (at the upper-left corner).

8. (Optional) Bookmark this page in your browser for future use.

   You can use the bookmarked URL to log in to Network Director without logging in to Junos Space first.

Discovering Devices

When you start Network Director for the first time, the system does not have any devices. The first step is to build your network. Even with large networks, Network Director has made this step relatively easy and straightforward. You will add devices to Network Director and the database by using a process called *device discovery*. Once a device is discovered, it shows in the interface and Network Director begins to monitor the device.

Network Director provides a wizard for device discovery. The following example shows the path for device discovery through the wizard. For an alternate path, you can get a step-by-step instruction from the help system.

In this example, we provide an IP address range, and Network Director populates the database with all supported devices within that range.

1. While in the **Build** mode, select **Logical View**, **Location View**, **Device View**, or **Custom Group View** from the View selector.

   > **NOTE:** Select **Datacenter View** if you want to view and manage data centers by using Network Director. You must set up a data center from the Datacenter View. Network Director automatically discovers and adds devices that are part of the data center set up to its inventory. There is no separate device discovery task for the Datacenter View. You can also add devices that are discovered from the other views to a data center by editing a data center in the Datacenter View.

2. To discover physical devices, click **Discover Devices** in the Tasks pane. Each mode has a Tasks Pane that displays the actions you can take while in that mode and that particular network view.

3. (Optional) Type a name for the discovery job. The default name is ND Discovery.

4. Click **Add** in the Device Targets window. You can add a single device IP address, a range of IP addresses, an IP subnet, or a hostname. In this example, we select an IP address range.

5. Provide the initial or the lowest IP address value and the ending or highest IP address value for the range and click **Add**. You can have up to 1024 devices in a range. After you click Add, the address range is listed in the Device Targets window.

6. Click **Next** or click **Discovery Options** to proceed to specify the device credentials and method of discovery.

7. Click **Add** in the Device Credentials window and enter the username and password assigned for administrative access.

8. Select **Ping**, **SNMP**, or both as the method of device discovery. Selecting both is the preferred method if the device is configured for SNMP.

   NOTE: Only SNMP version 3 is supported in FIPS mode.

   If you select SNMP, the Add SNMP Settings dialog box is displayed. In this example, because we run SNMP version 3, we need to provide the community string. Click **Add** to save the setting.

   NOTE: You cannot choose a method for device discovery for virtual network discovery.

9. Click **Next** or **Schedule Options** to proceed to schedule the time when discovery is run.

   NOTE: Scheduling options are not available for virtual network discovery.

10. Indicate whether to run the device discovery now or set up a schedule to minimize network traffic. In this example, we set the schedule to run during off hours.

11. Click **Review** to review the settings before you exit the wizard.

12. Click **Finish** to complete the discovery setup and to save the settings.

13. Click **View Discovery Status** to view all scheduled and completed jobs. After a job completes, you can click **Show Details** to view further information on any unexpected results.

Installing Hot Patch

Network Director hot patches are signed using SHA256 and it should be installed using a script. The script validates the signature of the hot patch and triggers hot patch execution.

Run the following script to install the hot patch:

```
sh /var/www/cgi-bin/installAppHotpatch.sh -f <ND_HOTPATCH_IMAGE> --patch-script
<HOT_PATCH_SCRIPT>] [ARGUMENTS_TO_HOTPATCH_SCRIPT]
```

Logging In to Network Director

You connect to Network Director using your Web browser. The following Web browsers are supported: Internet Explorer versions 8.0 and 9.0, Mozilla Firefox version 3.6 or later, and Google Chrome version 17 and later. The minimum screen resolution is 1280 x 1024.

You can connect to Network Director one of two ways:

- Log in to Network Director directly by using the following URL:

  ```
  https://<n.n.n.n>/networkdirector
  ```

  where *n.n.n.n* is the IP address of the Junos Space Web interface. You can bookmark the login page for future use.

- Log in to Junos Space first by using the following URL:

  ```
  https://<n.n.n.n>/mainui
  ```

  where *n.n.n.n* is the IP address of the Junos Space Web interface.

  You can then switch to the Network Director interface by selecting Network Director from the Applications list in the left pane of the Junos Space user interface.

4

CHAPTER

Working in Build Mode

Discovering Devices in a Physical Network | 73

Managing the Topology View | 80

Discovering Devices in a Physical Network

IN THIS SECTION

- Specifying Target Devices | 74
- Specifying Discovery Options | 76
- Specifying Schedule Options | 78
- Reviewing Device Discovery Options | 78
- Viewing the Discovery Status | 79

You can discover and synchronize physical devices such as EX Series switches, QFX Series devices, MX Series routers, and wireless LAN controllers in your network that are managed by Network Director.

You can also discover and manage virtual devices in your virtual network from Network Director. To discover devices in your virtual network, follow the steps described in *Discovering Devices in a Datacenter Network*.

NOTE: To discover wireless LAN controllers and access points, Network Director connects to port *8889* of the wireless LAN controller for sending an *HTTPS* request to the controller. Therefore, port *8889* must be open on the wireless LAN controller for Network Director to discover wireless LAN devices. From the Junos Space JA2500 Appliance or the Junos Space Virtual Appliance, you can verify the availability of port 8889 using the CLI command **root@space# nmap <IP address of controller> -p 8889**.

On EX Series switches, Network Director connects to port *22* (the default port) on the Junos Space JA2500 Appliance or the Junos Space Virtual Appliance by using SSH. You can configure port *22* on the Junos Space appliances through **Administration** > **Applications** on the Junos Space Platform page. Select **Network Application Platform** and click **Actions** > **Modify Application Settings**. Change the SSH port for device connection to *22*.

Device discovery is a three-step process in which you specify the target devices, the discovery options, and the schedule options.

While in Build mode, from the Tasks pane, click **Discover Devices** from the Device Discovery menu. The Discover Devices page is displayed.

This topic describes:

Specifying Target Devices

You can add devices to Network Director for device discovery by clicking either **Import from CSV** or **Add** , or both together. Click **Import from CSV** to add devices in bulk. You can add a large number of devices to Network Director by using a CSV file that contains information extracted from an LDAP repository. During device discovery, you can associate the devices with logical, location, and custom groups. You can list all devices to be discovered in the CSV file along with their logical, location, and custom groups. This eliminates the need to make an explicit association later. If you do not assign groups to the devices, the devices are added to the Unassigned folder by default. You can also change the assignment later. Associating new devices with groups makes the network simpler to manage and maintain.

To specify the target devices that you want Network Director to discover:

1. Enter a name for the device discovery job.

   The default name is ND Discovery.

2. To add devices in bulk, click **Import from CSV** from the Device Targets window.

   The Upload CSV File dialog box is displayed.

3. Click **Browse**.

   The File Upload dialog box is displayed.

4. Navigate to the target CSV file on your computer, select the file, and click **Open**.

   The CSV File Upload dialog box reappears, this time displaying the name of the selected file.

   > **NOTE:** The selected CSV file must follow the same file format as that of the sample CSV file.

5. Click **Upload** to upload the selected CSV file.

6. To add individual devices by specifying the IP address credentials, click **Add** in the Device Targets table.

   The Add Device Target dialog box appears.

7. In the Add Device Target dialog box, perform the following steps:

   a. Choose one of the following options to specify target devices:

- Select the **IP** option and enter the IP address of the device.
- Select the **IP-Range** option and enter a range of IP addresses for the devices.

  The maximum number of IP addresses for an IP range target is 1024.
- Select the **IP-Subnet** option and enter an IP subnet for the devices.
- Select the **HostName** option and enter the hostname of the device.

b. In the Assign To section, specify the following groups to which the newly discovered devices can be assigned:

- From the Logical Group drop-down menu, select **Core**, **Aggregation**, **Access**, or **Layer 3 Fabric** to specify the logical grouping of the device.

  Select the Layer 3 Fabric option to discover a Layer 3 fabric that is not created using Network Director and OpenClos. You can discover devices in Network Director that belong to the same IP subnet. To discover a Layer 3 Fabric, specify the IP subnet range, as all the devices that belong to the same Layer 3 Fabric resides in the same subnet. Network Director expands the IP subnet range and reaches every single IP address that you have specified in the IP range.

  Network Director initially discovers the Layer 3 Fabric based on the IP subnet and range. However, you can manually discover Layer 3 Fabric at a later stage by entering the host name of the Layer 3 Fabric.
- For the Location Group field, click **Select** to choose the location group for the device or input the location path for the association. To clear the selection, click **Clear**.

  Use the following format for the location path for the respective associations:

  - *site-name*#S/*building-name*#B
  - *site-name*#S/*building-name*#B/*floor-name*#F#*floor-level*
  - *site-name*#S/*building-name*#B/*floor-name*#F#1 - 1st level
  - *site-name*#S/*building-name*#B/*floor-name*#F#*floor-level*/*closet-name*#C
  - *site-name*#S/*building-name*#B/*floor-name*#F#*floor-level*/*aisle-name*#A/*rack-name*#R
  - *site-name*#S/*outdoorarea-name*#O

  If the location paths do not point to existing locations in Network Director, new location groups are created before the devices are assigned to them.
- For the Custom Group field, click **Select** to choose the custom group for the device or input the custom group path. To clear the selection, click **Clear**.

  Use the following format for the custom group path:

  - *customgroup1-name*/*customgroup2-name*

If the custom group paths do not point to existing custom groups, new groups are created before the devices are assigned to them.

c. Click **Add** to save the target devices that you specified, or click **Add More** to add more target devices. When you have added all target devices that you want Network Director to discover, click **Add**.

The Discover Targets table displays the addresses of the configured target devices.

8. Following device discovery management options are available:
   - To edit a target device, select a row from the Device Targets table and click **Edit**. Make the required changes and click **Add** to display the IP addresses in the Device Targets table
   - To delete a target device, select a row from the Device Targets table and click **Delete**.
   - To view and download a sample CSV file, click **CSV Sample**. The Opening Device_Discovery_CSV.csv file dialog box is displayed. You can open the sample CSV file or save the sample CSV file.
9. Click **Next** or click **Discovery Options** from the top wizard workflow to go to the Discovery Options page. Specify the options as described in "Specifying Discovery Options" on page 76.

Specifying Discovery Options

To add the device credentials and specify the probes:

1. Add the device credentials. To add the credentials, click **Add** from the Device Credentials table.

   The Add Device Credentials dialog box is displayed.

   > **NOTE:** If the credentials were specified in the CSV file, the Credentials table displays those values. If the credentials were not specified in the CSV file, then enter the values in the Add Device Credentials dialog box.

   - Specify the administrator username and password, and confirm the password. The username and password must match the name and password configured on the device. The username is a mandatory field.
   - Click **Add** to save the username and password that you specified or click **Add More** to add another username and password.

     Click **Add** after you have finished adding all login credentials. The Device Credentials table displays the usernames that you configured.
2. Specify the probes from the Specify Probes table. Select a probe method to discover the target devices.

> **NOTE:** Only SNMP version 3 is supported in FIPS mode.

- Select **Use Ping** if SNMP is not configured for the device and clear the **Use SNMP** check box.

  Network Director uses the Juniper Networks Device Management Interface (DMI) to directly connect to and discover devices. DMI is an extension to the NETCONF network management protocol.

- Select **Use SNMP** if SNMP is configured for the device, and clear the **Use Ping** check box.

  Network Director uses the **SNMP GET** command to discover target devices.

- Select both the **Use Ping** and the **Use SNMP** check boxes, to enable Network Director for faster discovery of the target devices, provided the device is pingable and also SNMP is enabled on the device.

> **NOTE:** Network Director uses the Juniper Networks Device Management Interface (DMI) adapter to manage devices that do not run Junos OS. Wireless LAN controllers are not DMI-complaint and use the MSS software. However, if you enable Use SNMP, Network Director detects whether the device is running a DMI-complaint software or not. The controllers always use a DMI adapter and hence can be detected.
>
> If you have not enabled Use SNMP, then Network Director assumes that all devices that failed during device discovery are controllers and retry the process if the port 8889 is open.

3. Click **Add** if you have selected the Use SNMP check box.

   The Add SNMP Settings dialog box is displayed.

   Select either **SNMP V1/V2C** or **SNMP V3**. Based on the selection, you need to enter the details as follows:

   - If you selected SNMP V1/V2C, specify a community string, which can be *public*, *private*, or a predefined string.

     Click **Add** in the Add SNMP Settings dialog box or click **Add More** to add more strings to the community. If you click **Add More**, when you are done adding all the strings, click **Add** to save the SNMP settings for V1/V2C.

   - If you selected SNMP V3:
     - Enter a username
     - Select the privacy type (AES 128, DES, or None).
     - Enter the privacy password (if AES 128 or DES). If you specify none for the privacy type, the privacy function is disabled.

- Select the authentication type (MD5, SHA, or none).
- Enter the authentication password (if MD5 or SHA). If you specify none for the authentication type, the authentication function is disabled.
- Click **Add** to save the SNMP settings and close the dialog box, or click **Add More** to add additional configurations. If you clicked Add More, click **Add** to save the settings and close the dialog box.

The Specify Probes table displays the configured SNMP settings.

4. Click **Next** or click **Schedule Options** from the top wizard workflow to go to the Discovery Schedule Options page. Specify the options as described in the "Specifying Schedule Options" on page 78.

Specifying Schedule Options

To specify the scheduler details:

1. Click **Run Now** if you want to discover the devices immediately or Click **Schedule at a later time** if you want to schedule the device discovery for a future time.

   If you select **Schedule at a later time**, specify the date and time to run the device discovery.

2. Click **Next** or click **Review** from the top wizard workflow to view the configuration. See "Reviewing Device Discovery Options" on page 78.

Reviewing Device Discovery Options

From this page, you can save or make changes to the device discovery options.

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

  Alternatively, you can click the appropriate buttons in the profile 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.

- Click **Finish** when you are done with the configurations.

  A message window opens, displaying the status of the device discovery job name and job ID. Click **OK**.

  The Device Discovery Jobs page is displayed with the list of jobs scheduled.

Viewing the Discovery Status

After you have configured the device discovery options, you can view the device discovery status from the **View Discovery Status** option from the **Device Discovery** menu.

The **Device Discovery Jobs** page displays all the scheduled device discovery jobs. You can view the following details from the Device Discovery Jobs page as described in Table 10 on page 79.

Table 10: Viewing Device Discover Jobs

Field	Description
Job ID	An identifier assigned to the job.
Job Name	The name of the job (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 displayed 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 displayed if all of the devices in the job completed successfully.
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the job.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a job, select the check box against Job ID or Job Name and click **Show Details**. The Discover Network Elements window displays details of the device discovery job.

NOTE: During device discovery, if Network Director is unable to read the device configurations, then the status displays Failed state. For such failures, you can check the reason for failure from the Manage Jobs page in System mode. You must make the required changes to the device configuration using the CLI so that Network Director can read the configuration. Network Director automatically resynchronizes once you enable a device discovery job. If Network Director cannot discover the device even after resynchronization, then you must rediscover the device after making the appropriate changes in the device configurations by using the CLI.

Managing the Topology View

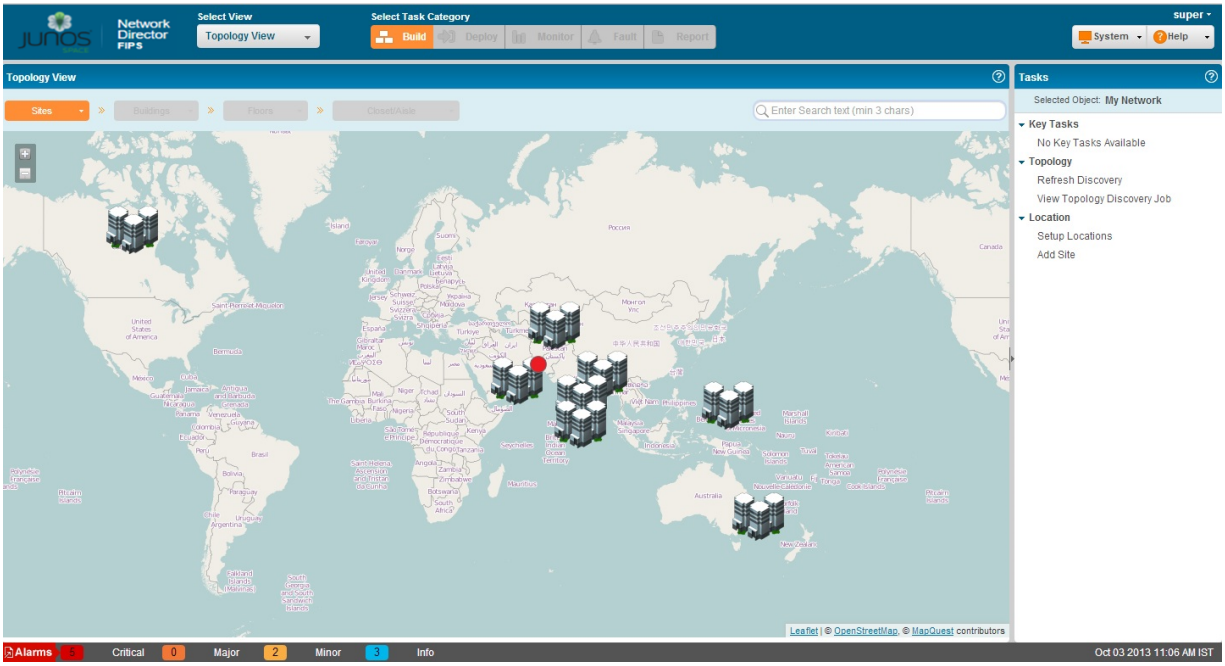
IN THIS SECTION

- Viewing the Network Topology | **81**
- Refreshing the Topology | **83**
- Viewing Topology | **84**
- Viewing Topology Discovery Job | **85**
- Setting Up Locations | **86**
- Viewing the Alarm Details | **86**
- Discovering the Linux Hosts | **86**
- Displaying Device Connectivity | **87**
- Displaying QFabric Connectivity | **91**
- Displaying Virtual Chassis and Virtual Chassis Fabric Connectivity | **94**
- Displaying Virtual Network Connectivity | **97**
- Displaying Third-Party Device Details | **97**
- Uploading Floor Plans | **98**
- Uploading Topology Map | **99**

Viewing the Network Topology

Topology View enables you to view all the discovered devices in your network, overlaid on a map. You can create sites, buildings, floors, outdoor areas, closets, and racks by using the Location wizard in Topology View. You can use the Topology View to zoom in or zoom out of a site or a building. You can also see the connectivity between a device and its immediate neighbors, alarms details, port details, and so on. An example of how the topology map looks like after you have added the location details is shown in Figure 9 on page 81.

Figure 9: Main Topology Window



The topology display is created by layering the device images on top of the imported floor plan images.

In addition to the tasks outlined in the *Topology View Tasks*, you can perform the following tasks from the Topology View pane:

- Zoom In and Zoom Out—You can use the zoom in ( ) or zoom out( ) buttons to get a detailed or high-level view. Network Director enables you to zoom in and view details up to the rack level, if you have defined racks and assigned devices to the rack.
- Pan—Network Director enables you to pan the topolog. You can move the devices to different parts on the topology by holding the mouse button down and dragging to a specific part of the map.

  Network Director displays the sites, buildings, and geographical coordinates on the topology map based on the address specified while setting up the locations. However, you can move the devices around to another location by selecting, dragging, and dropping the device to the correct location. For example, you can move a site from a US site to a Bangalore site on the topology by using the Pan feature. This

helps to determine the correct location of a site because while setting up the location details, it is not mandatory to provide the address information.

- Search and Locate—You can search for all nodes such as sites, building, floors, specific devices, all devices in a floor, and so on by entering a search keyword or the complete name of the device in the Search field. On entering the search criteria, you might see the list of nodes or just one node based on the search criteria. When you select the node, Network Director locates the node and Topology View is panned to ensure the selected node is centered on the page. In cases where a device is at the edge of the map the corner is aligned accordingly to bring device in view.
- View details—If you mouse over a entity (site, building, device), the entity gets highlighted and Network Director displays details such as the building name or IP address and the number of active alarms on that entity. A colored dot that appears on the upper right corner of the entity identifies whether there are alarms on the entity and the color of the dot indicates the severity level of the alarm. See Table 11 on page 82 to know more about the alarm severity indicator for each alarm severity.

Table 11: Alarm Severity Indicator

Alarm severity	Indicator
Critical	
Major	
Minor	
Informational	

NOTE: Each of these entities might have alarms of different severities. Network Director displays the indicator based on the most severe alarm on an entity. For example, if a device has 3 informational alarms and one major alarm, Network Director displays the indicator for the major alarm ( ).

- Highlight and select View Device Connectivity—Select a device and click **View Device Connectivity**, **View QFabric Connectivity**, **View VC/VCF Connectivity**, or **View Virtual Network Connectivity** to view the selected device's connectivity with other devices. Each of these tasks, except the **View Device Connectivity**, are visible only when you select a device that is part of a QFabric system, Virtual Chassis, Virtual Chassis Fabric, or a Virtual network. The device images are displayed along with details such as name, IP address, and the connectivity link between the devices.
- Navigation—Use the navigation breadcrumbs at the top of the page to navigate through sites, buildings, floors, closets, or aisles. For there are more than one entities at any give level, you can use the Down

arrow in the breadcrumb to navigate to that entity. For example, if you want to navigate from floor-1 in building-1 to floor-3 in building-2, you can use the down arrow in the building breadcrumb to select building-2 and the down arrow in the floor breadcrumb to select floor-3.

- Host Information—You can use the + button to expand the members to view the host details. You can also view the virtual machines if the host is a hypervisor and managed by Network Director.

Refreshing the Topology

You can refresh the devices discovered and managed by Network Director from the Tasks pane in the Topology View and the Datacenter View. You can add the Refresh Topology task to the Key tasks in both the views if you will use this task frequently.

To refresh the device discovery process:

1. Click **Refresh Topology** from Key Tasks or the Topology View, or from the Datacenter Discovery panes.

   The Refresh Discovery window is displayed along with the SNMP details that you specified in the discovery options in the Device Discovery task page.

   If you have not specified the SNMP details while discovering the devices, proceed to Step 3.

2. Select the **SNMP version** from the SNMP version table and click **Discover**. The Refresh Topology window appears displaying the progress of the topology discovery.

3. If SNMP version details are not displayed in the SNMP version table, click **Add** on the Refresh Discovery window.

   > **NOTE:** Only SNMP version 3 is supported in FIPS mode.

   The Add SNMP Settings dialog box is displayed.

   Select **SNMP V3**, specify the following:

   - Enter a username.
   - Select the privacy type (AES 128, AES 192, AES 256, or None).
   - Enter the privacy password.
   - Select the authentication type (SHA1).

- Enter the authentication password (SHA1).
- Click **Add** to save the SNMP settings and close the dialog box, or click **Add More** to add additional configurations. If you clicked Add More, click **Add** to save the settings and close the dialog box.

The specified details are displayed in the SNMP version table.

4. Click **Discover**.

   The Refresh Topology window is displayed, showing details of the device discovery.

Viewing Topology

The Refresh Topology window displays the refresh device discovery job details as described in Table 12 on page 84.

Table 12: Refresh Topology Job Details

Field	Description
Job Name	The Refresh topology job name along with the Job ID.
Start Time	The time at which the refresh discovery job is initiated.
End Time	The time at which the refresh discovery job is completed.
Percentage Progress	Displays the progress of the job in percentage. When the job is completed, displays 100 percentage.
Status	The status of the job. The status is *In Progress* until the job is completed.
Target Devices Count	The total number of targets for the discovery of devices.
Discovered Devices Count	The total number of discovered devices for which the SNMP parameters are specified. **NOTE:** In the Topology View, you can view the network connections of only those discovered devices for which LLDP, SNMP, and STP parameters are set.
Discovered Subnets Count	The total number of subnets discovered.
Targets	The Targets table displays the Management IP addresses of the devices discovered along with the status of the discovery process.

Use the right and left arrows to navigate through the discovered pages. You can specify the details to be displayed in a page by selecting the **show items** list box and specifying the number of items to be displayed in one page.

Click **Close** to close the Refresh Topology page and return to the main Topology page.

Viewing Topology Discovery Job

To view the discovery jobs in the Topology View and the Datacenter View, click **View Topology Discovery Job**. The Topology Discovery Jobs window opens displaying details of the topology related jobs as described in Table 13 on page 85. To view any hidden column, mouse over column heading, select the down arrow, and then click **Columns**. Select the check box to display the hidden columns.

Table 13: Job Details for Topology Discovery

Field	Description
Job ID	For each job-based task, the audit log includes a job ID.
Job Name	The name of the job.
Percent	The percentage of completion of the job.
State	The status of the job: • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started • In progress—Job is has started, but not completed • Cancelled—Job is cancelled
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the task.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a topology discovery job, select a row and click **Show Details**. To cancel a scheduled job, select a job that is scheduled for a later time or a job that is in progress and click **Cancel**.

Setting Up Locations

You can set up locations and assign devices to these locations by setting up the Location View. To set up Location View, see .

Viewing the Alarm Details

You can view the alarm details at site, building, floor, closet, aisle and rack levels. Based on the location node, the alarms are aggregated and displayed. That is, all the alarms for a particular building is aggregated and displayed at the building level. The alarms display as red, orange, yellow, and blue dots indicating critical, major, minor, and info alarms. Network Director updates and displays the alarm status changes in real time in the Topology view. To view the Alarm details for a device, navigate to the device level, select a device, and click one of the following options from Alarm in the Tasks pane:

- Show Alarms By Severity, see *Alarms by Severity Monitor*
- Show Alarms By Category, see *Alarms by Category Monitor*
- Show Alarms By State, see *Alarms by State Monitor*
- Show Current Active Alarms, see *Current Active Alarms Monitor*

Discovering the Linux Hosts

Based on the LLDP discovery method, you can discover the hosts for various Linux platforms such as Ubuntu, CentOS, and Red Hat by clicking **Refresh Topology**. You can also view the additional information in the tool tip that appears when you mouse over a host. These hosts also show icons that identify if a server is based on its respective platform. For example, if a server is a generic Linux server, a Linux icon is shown in the topology.

NOTE: You must enable LLDP both on the switch and on the host.

Displaying Device Connectivity

At the device level, you can view the connectivity details of a device and the details of all the devices that are connected to the specified device by using Topology View in Network Director. The Device Connectivity View also displays various details about the selected device and the immediate neighbors. The level of detail that Network Director displays in the Device Connectivity View differs based on the type of device that you select.

To view the connectivity details of a device:

1. Do one of the following:
   - While in the Logical, Location, Device, or Custom View, select the device for which you want to view connectivity from the View pane and click **Connectivity** > **View Device Connectivity** from the Tasks pane.
   - In the Topology View, navigate to a device in a building, floor, outdoor area, closet or rack and select the device for which you want to view the connectivity details and click **Connectivity** > **View Device Connectivity** from the Topology Tasks pane.

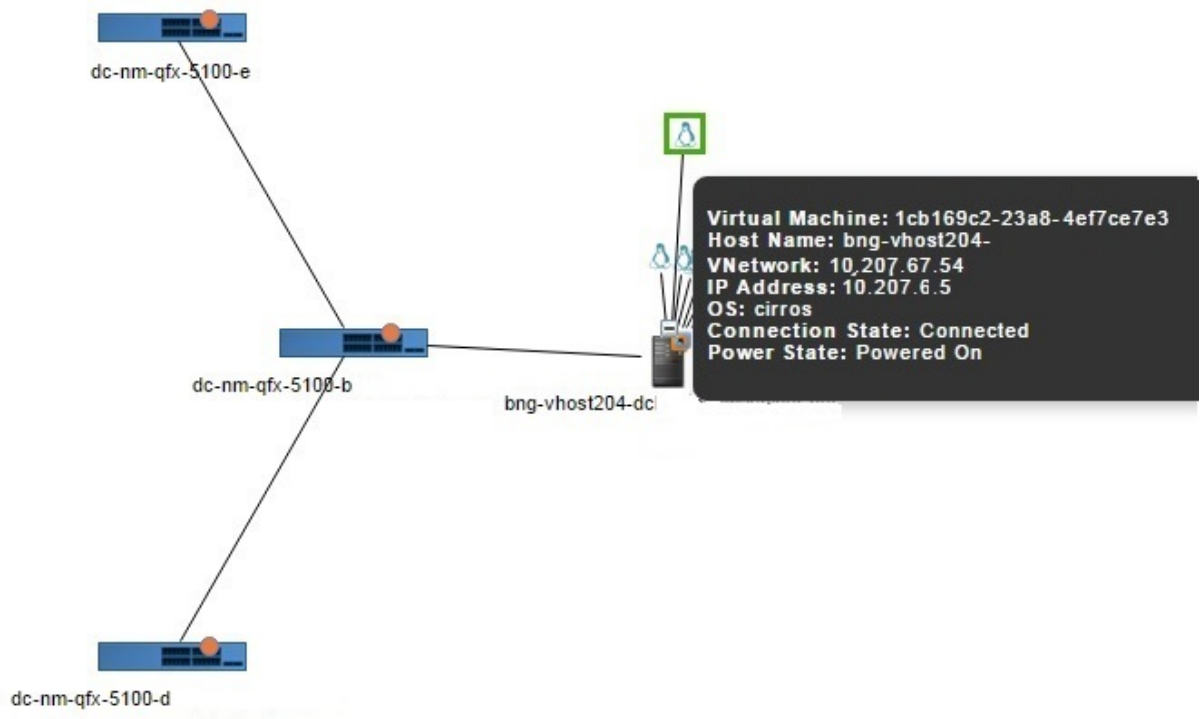
     NOTE: The Connectivity task container is available only after you select a device.

   The Device Connectivity page opens. You can view the device connectivity details either in graphical view or in grid view. The default view is the graphical view.

   In the graphical view, the device is displayed in the center and its network connectivity to all the connected devices are displayed as in Figure 10 on page 88. Mouse over a device to view details of the highlighted device.

   NOTE: If the selected device is connected to a device that is not a Juniper Networks device, the latter appears dimmed in the Device Connectivity page indicating that the device is not managed by Network Director.

Figure 10: Displaying the Connection Details in Graphical View



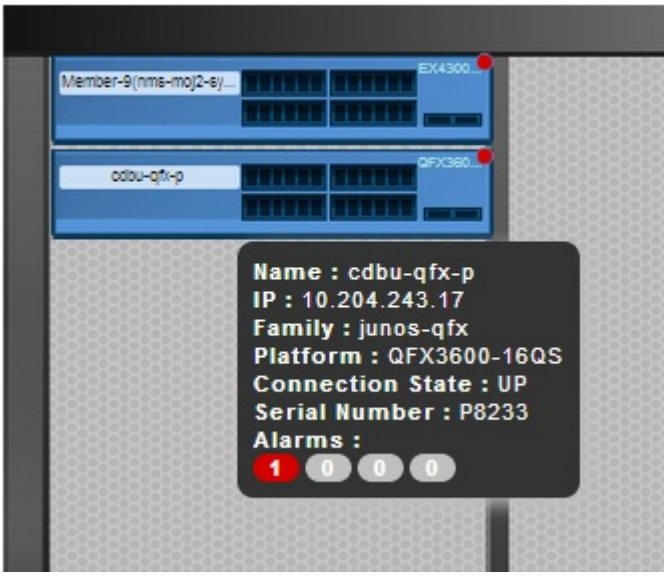
If the selected device is connected to more than sixty devices, then all the connected devices are highlighted in a circular form or a grid form. If the selected device is connected to less than 60 devices, then the links between the interconnected devices are displayed.

The device images are displayed along with details such as name, IP address, and alarm state information in colored labels that provide health and reachability information. You can also view the details of the hosts or virtual machines that are connected to the switches.

You can view the following details in the Device Connectivity - Graphical view:

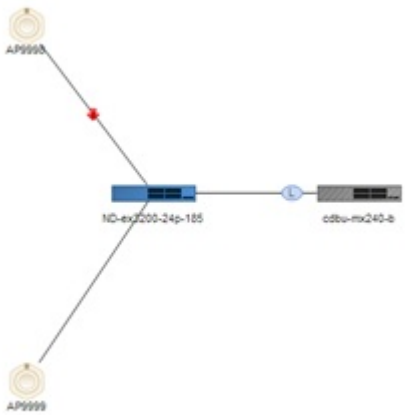
- Name—The name of the device provided while configuring the device. The device name is displayed as a label.
- IP—The IP address of the device.
- Family—The family or platform to which the device belongs to. Family can be an JUNOS-EX, JUNOS-QFX, JUNOS-QF, MSSOS, and WLC-AP.
- Serial Number—Serial number of the device.
- Alarms—The alarm details displaying the number of critical, major, minor alarms, or info for the device. Alarms details are color coded to indicate their severity level as shown in Figure 11 on page 89. Network Director updates and displays the alarm status changes in real time in the Topology view.

Figure 11: Alarm Indicator



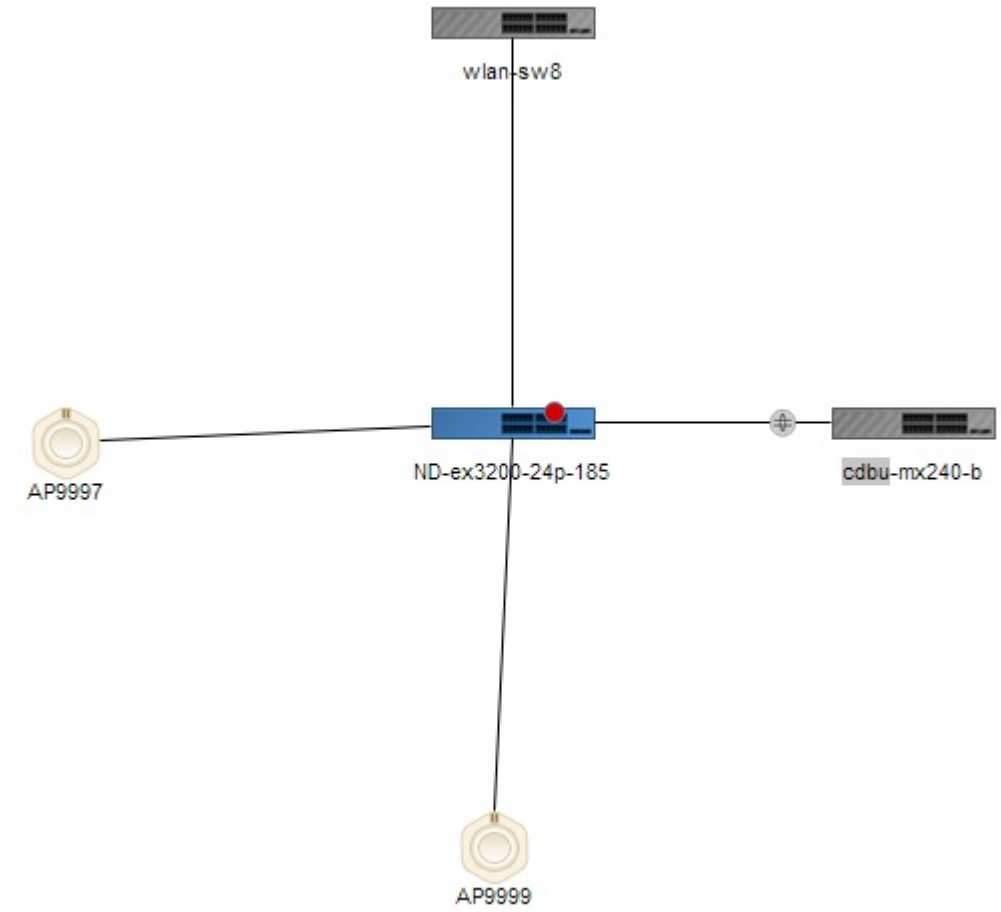
- Connection State—Connection status of the device. Connection state can be UP, DOWN or N/A. Network Director updates and displays the connection state changes in real time in the Topology view.
- Link status—Indicates whether the link between two devices is UP or DOWN as shown in Figure 12 on page 89. Network Director updates and displays the link status changes in real time in the Topology view.

Figure 12: Link Status Indicator



- LAG—Identifies connections that are configured as LAGs as shown in Figure 13 on page 90.

Figure 13: LAGs in the Device Connectivity view

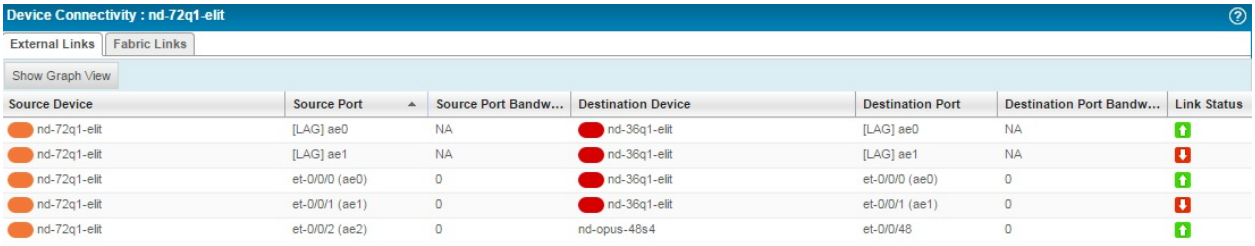


You can view the following details of the virtual machine that are connected to hosts:

- Virtual Machine—Name of the virtual machine.
- Host Name—Name of the host to which the virtual machine is connected to.
- VNetwork—Name of the virtual network.
- OS—Name of the operating system on which the virtual machine is running.
- Connection State—Connection status of the virtual machine. Connection state can be UP, DOWN or N/A.
- Power State—State of the power supply: Powered On or Powered Off.

2. Click **Show Grid View** to view the device connectivity details in a tabular format as displayed in Figure 14 on page 91.

Figure 14: Displaying the Connection Details in Grid View



The following details are displayed in the table:

- Source Node—Name of the device specified while configuring the device.
- Source Port—Source port of the device.
- Source Port Bandwidth %—Realtime percentage of bandwidth utilized at the source port.
- Destination Node—Name of the device or devices the device is connected to.
- Destination port—The port number on the destination device to which the source device is connected to.
- Destination Port Bandwidth %—Realtime percentage of bandwidth utilized at the destination port.
- Link Status—Indicates if the link to the device is UP or DOWN.

You can sort the details in the table in the ascending order or descending order for each column. You can also use filters to display only the desired device connectivity details.

Displaying QFabric Connectivity

You can view the QFabric devices available in your network by navigating to the rack, closet, or floors from the Topology View. Alternatively, you can search for the QFabric devices by entering a search criteria in the Search field. You can also assign the QFabric devices to a rack, closet, or floor from Topology View.

Network Director enables you to view the data plane topology and the control plane topology from the Fabric Connectivity page. Data plane is a redundant, high-performance, and scalable data plane that carries QFabric system data traffic. Control plane constitutes of the internal network connection that carries control traffic between the various QFabric system components such as node devices, interconnect devices, director group processes, and the control plane Ethernet switches.

You can view the connection details of the QFabric Interconnects with the nodes by using all views except the Dashboard View and Datacenter View.

To view the connection details of the QFabric devices:

Do one of the following:

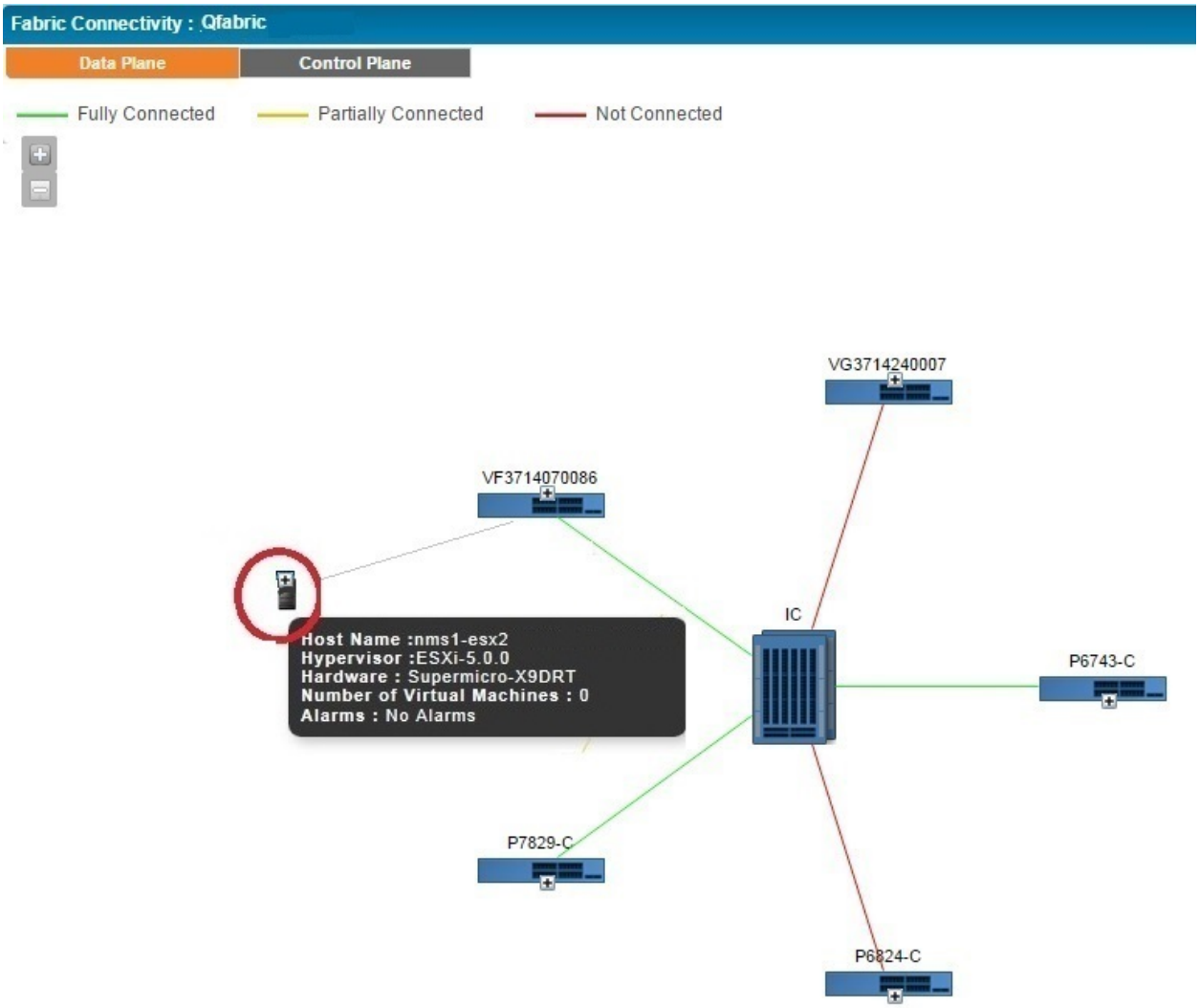
- While in the Logical, Location, Device, or Custom View, select the device for which you want to view the QFabric connectivity from the View pane and click **Connectivity** > **View QFabric Connectivity** from the Tasks pane.
- In the Topology View, navigate to a device in a building, floor, outdoor area, closet or rack and select the device for which you want to view the connectivity details and click **Connectivity** > **View QFabric Connectivity** from the Topology Tasks pane.

> **NOTE:** The Connectivity task container is available only after you select a device.

Click **Connectivity** > **View QFabric Connectivity** from the Tasks pane. Network Director displays the QFabric connectivity in the Data plane—with the interconnect in the center surrounded by the nodes—as shown in Figure 15 on page 93. Mouse over a device to view the port details and the connection state of that device.

By default, Network Director displays the Data plane topology for the selected QFabric. To view the control plane topology, click **Control Plane**.

Figure 15: Displaying the Data Plane Connectivity for a QFabric Switch



In the Figure 15 on page 93, the connection details are represented by green, yellow, and red lines.

- The green line indicates that the node is connected to all the Interconnects properly and all functions are normal.
- The yellow line indicates that the node is only partially connected to the Interconnect. That is, the node might be connected to some of the interconnects, but not all.
- The red line indicates that the node is not connected to any of the interconnects.

The following details are displayed for each device, if the details are configured on the device:

- Name of the device provided while configuring the device. The device name is displayed as a label.
- Platform of the device. Platform can be QFX3500, QFX3600, or QFX5100 switches.
- Node group name. The name of the node group to which this device belongs to.

- Node group type. The server name of the node group to which this device belongs to.
- Source Port—source port of the device.
- Destination port—The port number on the destination device to which the source device is connected to.

The following details are displayed for each host that is connected to the member:

- Host Name—Name of the host machine connected to the member.
- Hypervisor—Name of the hypervisor, which is used to create multiple virtual machines on a hardware device.
- Hardware—Type of hardware on which the hypervisor is deployed.
- Number of Virtual Machines—Number of the virtual machines that are connected to the hosts.
- Alarms—Number of active alarms on the device.

Displaying Virtual Chassis and Virtual Chassis Fabric Connectivity

You can view the connectivity between the components of Virtual Chassis and Virtual Chassis Fabric using the View VC/VCF Connectivity task. You can access this tasks from all views except Dashboard View and Datacenter View.

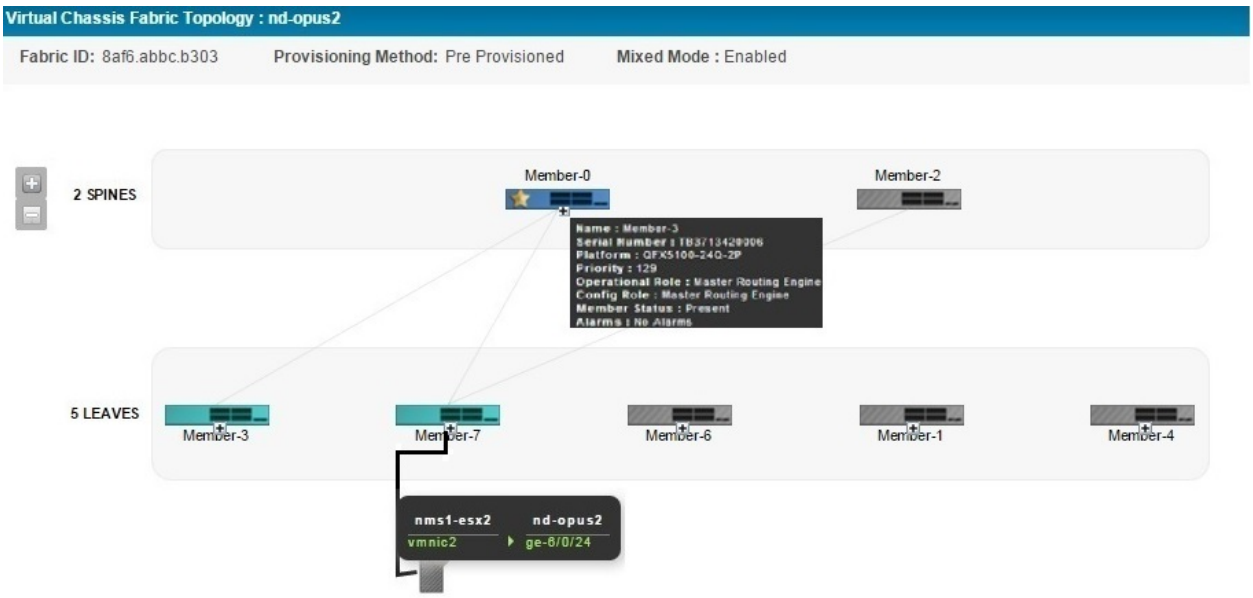
To view the connectivity details for a Virtual Chassis or a Virtual Chassis Fabric:

1. Do one of the following:
   - While in the Logical, Location, Device, or Custom View, select the device for which you want to view the Virtual Chassis or Virtual Chassis Fabric connectivity from the View pane and click **Connectivity** > **View VC/VCF Connectivity** from the Tasks pane.
   - In the Topology View, navigate to a device in a building, floor, outdoor area, closet or rack and select the device for which you want to view the Virtual Chassis or Virtual Chassis Fabric connectivity details and click **Connectivity** > **View VC/VCF Connectivity** from the Topology Tasks pane.

     NOTE: The Connectivity task container is available only after you select a device.

2. Click **Connectivity** > **View VC/VCF Connectivity** from the Tasks pane. Network Director displays the connectivity between the members of the selected Virtual Chassis as shown in Figure 16 on page 95. The inactive members and any members having alarms in down state are shown as grey icons in the topology identifying the state of the member. Mouse over a member to view details of that member.

Figure 16: Displaying the Connectivity for a Virtual Chassis Fabric



The following details are displayed in the top panel of the Virtual Chassis Topology View as shown in Table 14 on page 95.

Table 14: Common Details for the Virtual Chassis and Virtual Chassis Fabric

Details	Desciption
Fabric ID VC ID	All members of a Virtual Chassis configuration share one Virtual Chassis identifier (VCID). This identifier is derived from internal parameters.
Provisioning Method	The provisioning mode of the member. Provision mode can be *autoprovisioned*, *preprovisioned* or *not preprovisioned*. Autoprovisioning a Virtual Chassis Fabric (VCF) enables you to “plug and play” devices into your VCF after minimal initial configuration. In a VCF, you can have two to four members configured in the Routing Engine role. Of this, one member acts as the primary Routing Engine and another member acts as the backup Routing Engine. In a preprovisioned configuration, the selection of which member functions as the primary Routing Engine and which as the backup Routing Engine is determined by the software based on the primary-role election algorithm. In a configuration that is not preprovisioned, the selection of the primary and backup is determined by the primary-role priority value and secondary factors in the primary-role election algorithm.
VC Mode	Indicates whether the Virtual Chassis is mixed or not.

The following details are displayed in the Virtual Chassis Topology view for each member depending on the role of the member as shown in Table 15 on page 96.

Table 15: Details of VC/VCF Members

Details	Description	Role
Name	Name of the member switch provided while configuring the device. The device name is displayed as a label.	Primary Backup Line Card
Serial Number	Serial number of the member switch.	Primary Backup Line Card
Platform	Platform of the device. Platform can be QFX3500, QFX3600, QFX5100, or QFX5110.	Primary Backup Line Card
Priority	The primary-role priority value. This is the most important factor in determining the role of the member switch within the Virtual Chassis configuration.	Primary Backup Line Card
Operational Role	Operational role of the device. A device might be configured for a particular role, but can operate in the same or a different role. For example, a spine device configured with a Routing Engine role might operate as a line card. Therefore, the operational role of this device is Line Card. Operational role can be Routing Engine or Line Card.	Primary Backup Line Card
Config Role	The configured role of the device. This can be Routing Engine or Line card.	Primary Backup Line Card
Member Status	Displays the status of each member device: • Present—The device is connected and working fine. • Not Present—The device is not connected to the VC or VCF. • Inactive—The device is connected, but not running. • Non Provisioned—A configuration in which the roles of the members are assigned automatically; not configured statically (preprovisioned). • Pre Provisioned—A configuration that allows you to deterministically control the member ID and role assigned to a member by associating the member with its serial number.	Primary Backup Line Card

In addition to the above details, when you expand the host details, you can also view the details of the member and the link connected to the virtual machine.

Displaying Virtual Network Connectivity

To view the virtual network connectivity from Topology View, see .

Displaying Third-Party Device Details

Network Director now uses a unique icon to depict Samsung Access Points (APs) in the Device Connectivity page. You can mouse over the Samsung AP icon to view details of the device.

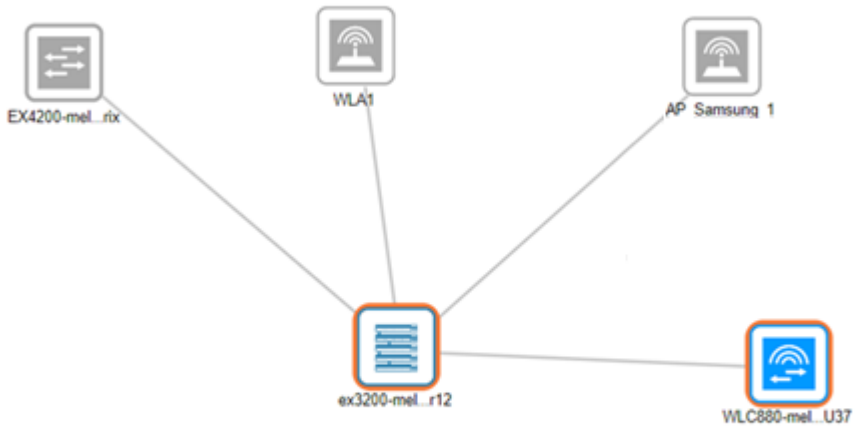
To view the Samung AP details:

1. From the View pane in the **Logical View**, **Location View**, **Device View**, **Custom View**, or **Topology View** , select the device for which you want to view the device connectivity.

2. From the **Tasks** pane, click **Connectivity > View Device Connectivity** .

   The Device Connectivity page opens showing the connectivity between various devices as shown in Figure 17 on page 97.

Figure 17: Samsung AP Device Connectivity



3. To view the Samsung AP details, mouse over the Samsung AP icon.

   A tool-tip, as shown in Figure 18 on page 98, is displayed showing the Samsung AP details listed in Table 16 on page 98.

Figure 18: Displaying Samsung AP Details

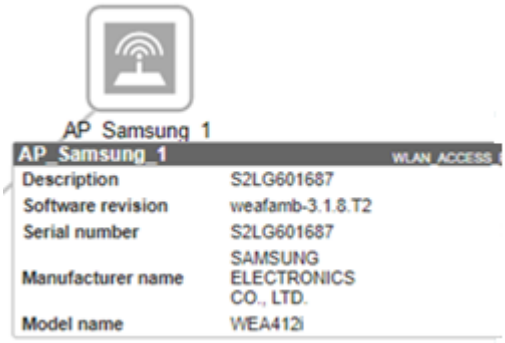


Table 16: Samsung AP Details

Field	Description
Name	The name of the device. The device name is displayed as a label.
Description	The description provided for the access point.
Software version	Software version that is running on the access point.
Serial number	Serial number of the access point.
Manufacturer name	Name of the access point manufacturer (Samsung Electronics CO., LTD.)
Model name	Model name of the access point.

NOTE: You can view the Samsung AP details that are connected to Juniper devices that runs Junos OS 12.1 version.

Uploading Floor Plans

You can upload the floor plan from the Topology View if you already have a floor plan for a specified building in a site.

To upload the floor plan:

1. Select a **Site** > **Building** > **Floor**. Alternatively, create a site, building, and floor. Click the **Upload Floor Plan** task from the Location task in the Tasks pane.

   The Upload Floor Plan dialog box is displayed.

2. Click **Browse** next to Image File to choose a floor plan file.

3. Navigate to the folder where you have saved the floor plan on your system and click **Open**.

4. Click **Upload** to upload the floor plan image.

5. Click **Cancel** if you do not want to upload the floor plan and quit the Upload Floor Plan dialog box.

Uploading Topology Map

You can upload a topology map for an outdoor area from the Topology View.

To upload the map:

1. Select a **Site** > **Outdoor area**. Alternatively, create an outdoor area within a site. Click the **Upload map** task from the Location task in the Tasks pane.

   The Upload Map dialog box is displayed.

2. Click **Browse** next to Image File to choose a map file.

3. Navigate to the folder where you have saved the topology map for an outdoor area on your system and click **Open**.

4. Click **Upload** to upload the topology map image.

5. Click **Cancel** if you do not want to upload the map and quit the Upload Map dialog box.

5
CHAPTER

Configuring Cloud-Based Datacenter Networks

Creating Data Centers Using Network Director

IN THIS SECTION

- Create a Data Center | 101
- View the Data Center Creation Status | 104
- Assigning Network Devices to a Data Center | 106

The cloud data center focuses on providing data center connectivity from various external networks to services located within a multitenant data center. You can discover, build, manage, and monitor your cloud data center from Network Director, using the Datacenter View. Network Director supports four types of cloud infrastructure providers—VMware vCenter, VMware vCenter with NSX plug-in, OpenStack, and OpenStack with NSX plug-in.

This topic describes the following:

Create a Data Center

To create a data center:

1. While in Build mode with Datacenter View selected, from the Tasks pane, click **Setup Datacenter** from the Datacenter Management menu. The Create Datacenter page opens.

2. In the Setup Datacenter wizard page, enter a name for the data center.

3. Click **Next** to specify details of the cloud infrastructure that the data center uses.

4. In the Cloud Infrastructure wizard page, do one of the following:
   - Click **No** if you do not want to specify a cloud infrastructure now or if your data center is a controller-less data center that uses only Juniper Networks devices. Skip to step 11.
   - Click **Yes** if you want to specify the cloud infrastructure for your data center.
5. Select the type of cloud infrastructure provider that the data center uses from the Cloud Infrastructure Provided box. You can choose VMware vCenter, VMware vCenter with NSX, OpenStack, and OpenStack with NSX as the provider.

6. Do one of the following:
   - Enter the IP address or the hostname of the vCenter or OpenStack server.
   - If you want to add a VMware vCenter that uses Platform Services Controller (PSC) location service, do the following:

     NOTE: PSC, a component of the VMware Cloud Infrastructure Suite, is available in VMware vSphere Version 6.0 or later. If your server is running an older version of vSphere, this step does not apply to you.

     a. Click **Search vCenter Using PSC Location Service**. The Search vCenter Using PSC Location Service window opens.

     b. Enter the IP address or the host name of the platform services controller.

     c. Click **Search vCenters**. Network Director displays all the vCenters that are managed by the PSC, in the list.

     d. Select a vCenter from the list and click **Select**. Network Director adds the vCenter that you selected to the Cloud Infrastructure wizard page.

7. Specify the port that Network Director uses to connect to the server. The default port used to connect to a vCenter server is 443 and that for an OpenStack Keystone service is 35357.

   NOTE: You can modify this and specify a port of your choice. If you do so, make sure to manually change the Junos Space firewall settings and apply to this port.

8. Specify the administrator username and password for the server you selected. The username and password must match the name and password configured on the server.

   NOTE: The administrator username that you specify for discovering the OpenStack server must have admin privileges and must belong to an admin tenant in the OpenStack server.

9. If you specified a vCenter server that is running VMware vSphere version 6.0 or later and would like Network Director to discover the virtual machines tags from vSphere, you must specify some additional settings. To do this, click **Additional Settings**. The vCenter Discovery Additional Settings window opens displaying the IP address of the vAPI endpoint (default value is the IP address or host name of the

vCenter server) and the port (default is 443) that Network Director uses to connect to the vAPI endpoint. If you plan to use an external PSC, you must specify the IP address of the vAPI endpoint and click **Update**.

Network Director closes the vCenter Discovery Additional Settings window.

> **NOTE:** If you specified the vCenter details by using the PSC location service as mentioned in step 6, Network Director obtains the vAPI details from the settings you specify. You need not specify the vAPI details as mentioned in this step.
>
> vAPI endpoint is a part of vCenter (running vSphere version 6.0 or later) that exposes APIs to new functionalities such as the tagging objects. Network Director leverages this functionality to obtain and display the virtual machine tag using the vAPI.

10. If you selected VMware vCenter with NSX or OpenStack with NSX as the provider, specify the following details about the NSX controller:

    a. Enter the IP address or the hostname of the NSX controller.

    b. Specify the port that Network Director uses to connect to the NSX plug-in. The default port used to connect to an NSX plug-in is 443.

    > **NOTE:** You can modify this and specify a port of your choice. If you do so, make sure to manually change the Junos Space firewall settings and apply to this port.

    c. Specify the administrator username and password for the NSX server. The username and password must match the name and password configured on the server.

    > **NOTE:** Enable Date Centre only with HTTPS TLSv1.2 configured with SHA256 RSA 2048 signature.

11. Click **Next** to specify the method that you want Network Director to use to build the data center network.

12. Select the Juniper Network devices that you want to add to the data center from the Available Devices table and click **>>** to add it to the Selected Devices table. You can also add data center fabrics such as a Layer 3 Fabric to your data center.

If you want to remove a device or fabric from the Selected Devices table, select the device or fabric and click **<<**.

13. To refresh the devices discovered and managed by Network Director, select the Refresh Topology check box. If you have not specified the SNMP details while discovering the devices or if you want to modify the SNMP details for the devices, click **Configure**. The Refresh Topology window appears. Specify the SNMP details by following the instructions given in the *Refreshing the Topology* section of *Managing the Topology View*.

14. Click **Done** to save the data center details.

    A message window opens, displaying the status of the cloud infrastructure discovery job name and job ID. Click **OK**.

    You can view the status of the discovery job in the Cloud Infrastructure Discovery Jobs page.

Network Director tries to discover the servers that you specified in the Cloud Infrastructure wizard page, if you specified the cloud infrastructure details. Network Director then adds the remaining network infrastructure based on the details you specified in the Network Infrastructure wizard page. Once these two steps are complete, Network Director lists that data center along with the devices that are part of the network infrastructure under My Datacenters in the View pane. You can perform various tasks on the data center by selecting the data center in the View pane.

View the Data Center Creation Status

After you have specified all the details in the Create Datacenter wizard and submitted it, you can view the discovery status from the View Cloud Discovery Status page in the Datacenter Management menu.

The Cloud Infrastructure Discovery Jobs page displays all the discovery jobs. From this page, you can view the details described in Table 17 on page 104.

Table 17: Cloud Infrastructure Discovery Jobs page Field Descriptions

Field	Description
Job ID	An identifier assigned to the job.
Job Name	The name of the job (user-created).
Percent	Percentage of the job that is complete.

Table 17: Cloud Infrastructure Discovery Jobs page Field Descriptions *(continued)*

Field	Description
Status	Job status. The possible states are: • CANCELLED—The job was canceled by a user. • FAILURE—The job failed. This state is displayed if any of the devices in the job failed; even if 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 displayed if all of the devices in the job completed successfully.
Summary	Summary of the job scheduled and executed with status. **NOTE:** If Network Director encounters an error while trying to retrieve the virtual machine tag, details about the error is displayed in this field.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the job.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a job, select the check box against **Job ID** or **Job Name** and click **Show Details**. The Discover Network Elements window displays details of the virtual network discovery job.

NOTE: During cloud infrastructure discovery, if Network Director is unable to read the device configurations, then the status is displayed as Failed. You can check the reason for the failure from the Manage Jobs page in System mode. You must make the required changes to the device configuration by using the CLI so that Network Director can read the configuration. Network Director automatically resynchronizes once you enable a cloud infrastructure discovery job. If Network Director cannot discover the device even after resynchronization, then you must rediscover the device after making the appropriate changes in the device configuration by using the CLI.

Assigning Network Devices to a Data Center

You can add network devices to a data center while you create a data center. Alternatively, you can skip this step while creating the data center and add network devices later by using the Assign Devices to Datacenter task.

To add network devices after you have created the data center:

1. While in Build mode with Datacenter View selected, select the data center to which you want to add devices in the View pane and click **Datacenter Management** > **Manage Network Infrastructure** from the Tasks pane. The Assign Devices to Datacenter page opens, listing the network devices that are discovered in Network Director.

2. Select one or more network devices that you want to add to the data center and click **Done**.

   Network Director adds the selected devices and updates the data center in the View pane.

6

CHAPTER

Working with Aruba Devices and Applications in Network Director

Linking to the Aruba Airwave Application | **108**

Linking to the Aruba Airwave Application

Sites with the Aruba Airwave application licenses can launch the Airwave application from within Network Director by supplying the Airwave application URL. After specifying the URL on the Wireless tab of Preferences, click **Launch Aruba Airwave** in Build mode, Monitor mode, Fault mode, or Report mode to load the respective pages of Airwave application.

To enable launching the Airwave application from within Network Director:

1. Type the URL required for launching the Airwave application.

   NOTE: Enable Aruba Airwave only with HTTPS TLSv1.2 configured with SHA256 RSA 2048 signature

2. Type the credentials that are used to log in to the Airwave application.

3. Specify the time in hours after which the Juniper Networks Network Director server synchronizes with the Aruba server to get the latest wireless devices inventory from the Aruba server.

   The default synchronize interval is 24 hours. You can enter upto 720 hours as synchronize interval.

   NOTE: If you specify the synchronize interval as 0 hours, the synchronization between the Juniper Networks server and Aruba server does not occur and you will need to manually synchronize these servers to retrieve the latest device inventory. To manually synchronize the servers click the **Resynchronize Now** button in the Aruba Wireless Device Inventory page.

4. Click **Check Connectivity** to check the network connection between the Aruba Aiwave application server and Network Director.

5. Click **OK**.

CHAPTER 7

Importing RingMaster Data

Importing RingMaster Data to Network Director | **110**

Importing RingMaster Data to Network Director

You can use the Import RingMaster Data task in the System Settings to import data from the network plan that is active in RingMaster. A network plan is a repository for all hardware, site, and configuration details for a single or multi-site wireless network. It can contain wireless network data that spans multiple sites or campuses, which include one or more buildings and associated floors, and possibly outdoor areas.

Network Director uses this data to discover devices, build profiles, configure the Location view, build the Topology view (including a floor plan, if one is defined in the network plan), and to assign devices to various entities in Location and Topology views.

Before you import RingMaster data to Network Director:

- Ensure that you have the correct network plan activated in RingMaster.
- Ensure that the RingMaster server is up and is accessible through the network.
- If your RingMaster server uses any port other than Port 443, then you must open that port from the Junos Space Network Management Platform server.

> **NOTE:** Enable RingMaster only with HTTPS TLSv1.2 configured with SHA256 RSA 2048 signature.

To import RingMaster data to Network Director:

1. From the Tasks menu in the Logical View, Location View, Device View or the Custom Group View, click **Device Discovery** > **Import RingMaster Data**.

2. Specify the RingMaster server details and user credentials of the user who has administrative access to the RingMaster server, in the appropriate fields.

3. Click **Import**. Network Director uses the details that you specified in this page to connect to RingMaster and start importing data.

After you click Import, Network Director performs the following tasks:

a. Imports the list of controllers and access points that are managed by the RingMaster server that you specified.

b. Initiates discovery of these controllers and access points.

c. Reads the configuration of the discovered devices.

d. Creates the necessary profiles based on the device configuration.

e. Assigns profiles to devices.

f. Performs location setup based on the location data that is available in the network plan.

g. Assigns devices to locations.

h. Imports floor plan, if defined, to the topology view.

You can use the Job Management page to track the progress of each of these tasks.