JUNIPER

NETWORKS®

Junos® Space

Network Director Quick Start Guide

Release
2.5

Modified: 2015-09-24

Table of Contents

Network Director Installation Overview

Junos Space Network Director is Juniper Networks' network management solution that empowers administrators to seamlessly manage Juniper Networks WLC Series Wireless LAN Controllers (WLCs), EX Series Ethernet Switches, EX Series switches with ELS, QFX Series switches, MX Series routers with ELS, QFabrics, and VMware virtual networks within a Junos Space application. Network Director provides a single interface for managing the entire management life cycle of the network, including configuration, device management, monitoring, fault management, and reporting. Before you install Network Director and the Network Director API, you must set up a Junos Space Appliance in a single-node configuration.

This Quick Start Guide describes how you can quickly set up a Junos Space Appliance in a single-node configuration, install Network Director and the Network Director API, and bring your devices under Network Director management.

You can install Network Director in one of the following hardware configurations:

- A 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

  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 Installing Juniper Networks Junos Space JA2500 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, 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, see Junos Space Virtual Appliance.

Follow all safety warnings and precautions as specified in General Safety Guidelines and Warnings.

The following sections describe the basic steps to install and configure Network Director and the Network Director API on a Junos Space JA2500 Appliance:

Installing a Junos Space Hardware Appliance for Network Director

The Juniper Networks Junos Space 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 number of appliances that can be connected together to form a management cluster will increase in subsequent releases in order to achieve even better horizontal scalability. The Junos Space architecture also achieves five nines availability.

The JA2500 appliance has a 2-U, rack-mountable chassis with dimensions of 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. In addition, 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 in a RAID 10 configuration. Two externally accessible cooling fans provide the required airflow and cooling for the appliance.

For detailed steps on installing a JA2500 appliance, see Installing Juniper Networks Junos Space JA2500 Appliance.

Follow all safety warnings and precautions as specified in *General Safety Guidelines and Warnings*.

Configuring Basic Junos Space Settings

The basic configuration procedure for setting up the hardware appliance to run as a single Junos Space node is summarized here. For complete configuration steps, see Configuring a Junos Space Appliance or Configuring the Basic Settings of a Junos Space Virtual Appliance.

You need two IP addresses on the same subnet to complete the configuration. The first IP address is for the eth0 interface on the appliance; the second IP address is for accessing Junos Space by using the Web GUI.

1. At the serial console login prompt, type the default username (**admin**) and press Enter.

2. Type the default password (**abc123**) and press Enter.

   You are prompted to change your password.

3. To change the default password, do the following:

   a. Type the default password and press Enter.

   b. Type a new password and press Enter.

   c. Retype the new password and press Enter.

   If the password is changed successfully, the message **passwd: all authentication tokens updated successfully** is displayed.

   > **NOTE:**
   > - All passwords are case-sensitive.
   > - A valid password must contain at least eight characters, of which at least three are of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters and must not contain a single uppercase letter at the beginning or only a single number at the end.
   >
   >   For example, Abcdwip9, Qc9rdiwt, and bRfjvin9 are invalid passwords, but AAbcdwip99, Qc9rdiwtQ, and bRfjvin99 are valid passwords.
   > - Alternatively, instead of using a string of characters, you can choose a passphrase that contains between 16 through 40 characters, and includes at least three dictionary words separated by at least one special character. For example, big#three;fork (contains 14 characters) and circlefaceglass (no special characters) are invalid while @big#three;fork& and circle;face;glass are valid.

4. Enter the new password to log in to the appliance.

5. Type **s** to proceed with the configuration of the appliance as a Junos Space node with full Junos Space Network Management Platform functionality. Every Junos Space installation requires at least one Junos Space node.

6. Select IPv4 or IPv6 as the option for IP addresses and specify the following details:

   a. Enter a new IP address for the interface eth0; for example, 10.10.20.15.

   b. Enter a subnet mask for the interface eth0; for example, 255.255.255.0.

> *i*
>
> NOTE: If you are configuring the appliance as part of a cluster (fabric), then all nodes in that fabric must be in the same subnet.
>
> For more information about the Junos Space fabric, see the *Fabric Management* chapter in the *Junos Space Network Management Platform User Guide* (available at http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html).

c. Enter the IP address for the default gateway; for example: 10.10.20.1.

> *i*
>
> NOTE: For detailed steps on configuring network settings, see Configuring a Junos Space Appliance as a Junos Space Node.

7. Enter the DNS name server address for the interface eth0; for example, 192.168.15.168.

8. Enter **n** as the response to the prompt: **Configure a separate interface for device management? [y/n]**.

9. Enter **n** as the response to the prompt: **Will this Junos Space system be added to an existing cluster? [y/n]**.

10. Enter the IP address for the Web server. This IP address must be in the same subnet as the IP address for the interface eth0, but a separate address; for example, 10.10.20.18.

11. Add an NTP server to synchronize the node with an external NTP source; for example, you can specify ntp.juniper.net as the external NTP server.

12. Enter the display name (logical node name) for this node; for example, tp-junosspace-01.

13. Enter the password for the appliance when it is in maintenance mode. The maintenance mode administrator must specify this password to access maintenance mode and shut down all nodes.

14. Reenter the password to confirm it. The system displays the settings summary.

    Settings Summary:

    > IP Change: eth0 is 10.10.20.15 / 255.255.255.0
    > Default Gateway = 10.10.20.1 on eth0
    > DNS add: 192.168.15.168
    > Create as first node or standalone
    > NTP add: ntp.juniper.net
    > Web IP address is 10.10.20.18
    > Node display name is "tp-junosspace-01"
    > Password for Junos Space maintenance mode is set.

    A> Apply settings
    C> Change settings
    Q> Quit and set up later
    R> Redraw Menu

Choice (ACOR):

15. Review the summary. If the settings are correct, enter **A** to apply the settings. The system initializes and the initialization messages appear before the system displays the Junos Space Appliance settings menu.

    Choice [ACQR]: A

    .
    .
    .
    Last login: Wed Feb 6 18:16:25 on ttyS0

    Welcome to the Junos Space network settings utility.

    Initializing, please wait

    Junos Space Settings Menu

    1> Change Password
    2> Set DNS Servers
    3> Change Time Options
    4> Retrieve Logs
    5> Security
    6> (Debug) run shell

    Q> Quit
    R> Redraw Menu

    Choice [1-6,QR]:

16. Type **Q** to quit the session. The configuration of the JA2500 Appliance is now complete.

Upgrading Junos Space

Network Director Release 2.5 is supported on Junos Space Network Management Platform Release 15.1R1. If your appliance is running the supported version of Junos Space, you can skip this procedure and begin installation of Network Director.

If your appliance is running a Junos Space release that is earlier than the supported release, you need to upgrade Junos Space before installing Network Director. To determine the Junos Space release version and to upgrade Junos Space, follow these steps:

1. Determine the installed Junos Space version:

    a. Log in to Junos Space by using the default username and password for Junos Space: **super** and **juniper123**.

       Junos Space opens the dashboard.

    b. Click the plus symbol **(+)** next to Administration to expand the Administration menu.

c. Click **Applications** to list all of the applications installed.

d. Note the version of the Network Management Platform or the Network Application Platform. (Some earlier versions of the Network Management Platform were named Network Application Platform.) If the currently installed release is a supported one, you can skip the rest of this procedure; if not, you must upgrade the Network Management Platform to a supported release.

2. Determine how many releases you need to install to bring the software up to minimum requirements.

   Junos Space supports upgrades from the last two versions. For example, Junos Space Release 13.1 supports upgrading from Release 12.3 or 12.2. Upgrades from releases still earlier require multiple steps.

3. Open a new browser page, log in to the Juniper customer support portal, and download the required Junos Space version to either the hard disk or to an SCP server. The Junos Space software images are located at http://www.juniper.net/support/downloads/?p=space.

4. Return to your Junos Space session after the download completes.

5. Upgrade Junos Space Network Management Platform to a supported release.

   Complete installation steps are provided at *How Do I Upgrade Junos Space?*.

Installing Network Director

Before you begin:

- If Network Director Release 2.5 is installed on the Junos Space Appliance, then you must uninstall it and restart JBoss before installing Network Director Release 2.5.

- Uninstall Junos Space Virtual Control, if it is installed on your Junos Space Network Management Platform. After uninstalling Virtual Control, you must run the clean up script before you proceed with the installation. You can download the cleanup script for Virtual Control from the Junos Space and Junos Space Network Director Download page.

- Download Network Director Release 2.5 software image to the hard disk or to an SCP server. Open a new browser page, log in to the Juniper software downloads page and download the required Network Director version to either the hard disk or to an SCP server. The Network Director software images are located at the Junos Space and Junos Space Network Director Download page.

To install Network Director from the Administration > Applications page of Junos Space:

1. Click the plus symbol (+) on the top left of the page.

2. Click either **Upload via HTTP** or **Upload via SCP** and upload the image as follows:

   To upload Network Director by using HTTP:

   a. Click **Upload via HTTP** to open the dialog box.

   b. Navigate to the local location where the Network Director or the Network Director API image is stored.

   c. Select the image file and click **Open** to load the path.

   d. Click **Upload** to load the image file into Junos Space.

   To upload Network Director by using SCP:

   a. Click **Upload via SCP** to open the Upload dialog box.

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

      • Enter the username.

      • Enter the password and reenter the password in the Confirm Password field.

      • Enter the host IP address.

      • Enter the local path name of the Network Director application file.

   c. Click **Upload** to load the image file into Junos Space.

3. Click **OK** to skip viewing the job results.

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

5. 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 inventory page. The new application also appears in the Application Chooser (at the upper-left corner).

6. Download the DMI schemas for devices that require a later schema, and upload the schema to the Junos Space. For more details, see "Uploading DMI Schemas" on page 15.

7. To work with Network Director, select **Network Director** from the Applications list in the upper left corner above the Tasks tree.

   Network Director starts in your browser window and opens the default view as shown in Figure 1 on page 8.

Figure 1: Network Director Interface
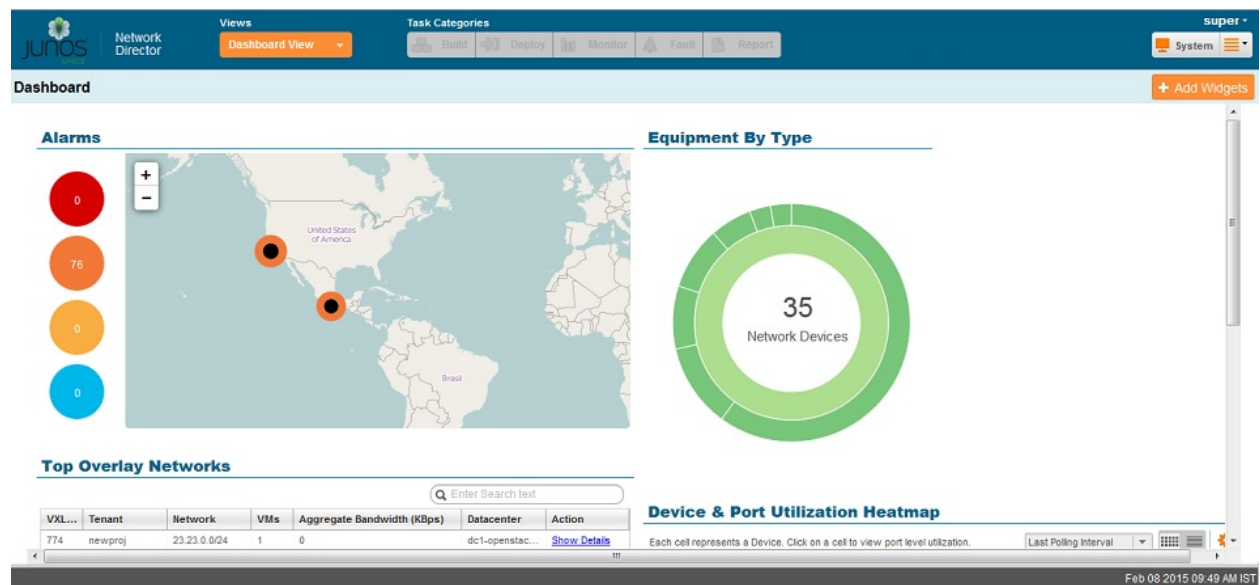
8. Bookmark this page in your browser for future use.

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

9. Do the following depending on your networking requirements:

   a. Perform the initial configuration of Network Director. See "Preparing Devices for Management by Network Director" on page 18.

   b. Install and configure Cloud Analytics Engine. See "Installing Cloud Analytics Engine" on page 14. Network Director uses Cloud Analytics Engine for network data analysis to improve application performance and availability.

Upgrading Network Director

You can upgrade Network Director from Release 1.6R1, 1.6R2, or 2.0 to Network Director Release 2.5. If your device is running a release of Network Director earlier than Release 1.6R1, you must first upgrade to Network Director Release 1.6R1, 1.6R2, or 2.0 and then follow the steps mentioned in this topic to upgrade to Network Director Release 2.5. For instructions on upgrading to Network Director Release 1.6R1, 1.6R2, or 2.0 respectively, see *Network Director Release 1.6R1 Quick Start Guide* , *Network Director Release 1.6R2 Quick Start Guide*, or *Network Director Release 2.0 Quick Start Guide*.

After resynchronizing device configuration (in Network Director), some of the profiles generated by Network Director are in unassigned state. To remove these profiles you must check the option **Purge unassigned system profiles after resynchronizing configuration** in System Preference page. However, while performing an upgrade to Network Director 2.5, the profiles that are in unassigned state cannot be removed by checking this option.

Before you start the upgrade, ensure that you have:

- Disabled monitoring for all categories in the Monitoring tab of the Preferences page. For more details, see Disabling Data Collection for Monitors.

- Taken a back up your database using the Junos Space backup feature. For more details, see Backing Up and Restoring the Database Overview.

- Junos Space Release 14.1R2.9 running on your appliance. If your appliance is running an unsupported release of Junos Space, you must upgrade Junos Space before installing Network Director. For step-by-step instructions on upgrading Junos Space, see "Upgrading Junos Space" on page 5.

- Downloaded the Network Director Release 2.5 software image to the hard disk or to an SCP server. The Network Director software images are located at http://www.juniper.net/support/downloads/space.html .

To upgrade Network Director from the **Administration > Applications** display of Junos Space:

1. Select Network Director from the list of installed applications and click **Upgrade Application** from the Actions menu.

2. In the Upgrade Application page, click either **Upload via HTTP** or **Upload via SCP** and navigate to the location where you stored the Network Director image.

   To upload Network Director by using *HTTP*:

   a. Click **Upload via HTTP** to open the dialog box.

   b. Navigate to the local location where the Network Director image is stored.

   c. Select the image file and click **Open** to load the path.

   d. Click **Upload** to load the image file into Junos Space.

   To upload Network Director by using *SCP*:

   a. Click **Upload via SCP** to open the Upload dialog box.

   b. Enter the Secure Copy credentials to upload the Network Director image from a remote server to Junos Space.

      - Enter the username.

      - Enter the password and reenter the password in the Confirm Password field.

      - Enter the host IP address.

      - Enter the local path name of the Network Director application file.

   c. Click **Upload** to load the image file into Junos Space.

3. Click **OK** to skip viewing the job results.

4. Select Network Director and click **Upgrade**.

   You can check the Job Status page to see the progress of the upgrade job. Once the upgrade completes, Network Director appears on the Applications inventory page.

The new or upgraded application also appears in the Application Chooser (at the upper-left corner).

5. After you upgrade Network Director, you must restart JBoss for the monitoring and fault features to work properly in standalone and cluster setups:

To restart the JBoss server in a standalone setup:

a. Stop the watchdog, domain controller, and JBoss services on the standalone node.

   service jmp-watchdog stop

   service jboss-dc stop

   service jboss stop

b. Start the watchdog service.

   service jmp-watchdog start

   > *i* NOTE: Starting the watchdog service restarts the JBoss and domain controller services as well.

   It takes approximately 20 minutes for the JBoss server to come up after the restart.

To restart the JBoss server in a cluster setup:

a. Stop the services on the secondary node.

   service jmp-watchdog stop

   service jboss stop

b. Stop the services on the master node (You can find the VIP hosted node Space > Fabric).

   service jmp-watchdog stop

   service jboss-dc stop

   service jboss stop

c. Start the services on the master node.

   service jmp-watchdog start

d. Start the service on the secondary node.

   service jmp-watchdog start

   It takes approximately 20 minutes for the JBoss server to come up after the restart.

6. Download the DMI schemas for devices that require a later schema, and upload the schema to the Junos Space. For more details, see "Uploading DMI Schemas" on page 15.

7. To work on Network Director, select **Network Director** from the Applications list in the upper left corner above the Tasks tree.

Network Director starts in the browser window. The default view is the Dashboard View. Use the View selector on the top banner to navigate to the other views—Logical View, Location View, Device View, Topology View, Custom Group View, or the Datacenter View.

8. 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.

Installing and Managing the Network Director Analytics Engine

The Network Director Analytics Engine enables Network Director to collect and analyze high-frequency statistics data from devices. QFX Series devices support the analytics feature that is required for generating high-frequency statistics data. Network Director uses this data to create network heat maps and monitor latency.

The Analytics Engine can run in the following modes:

- Integrated mode—The Analytics Engine runs on a Junos Space server. No additional hardware or software is required.

- External mode—The Analytics Engine runs on a separate, dedicated Analytics Engine server running CentOS.

This topic covers the following:

Running the Network Director Analytics Engine in Integrated Mode

The Analytics Engine is installed with Network Director. To run the Analytics Engine in integrated mode (on a Junos Space server), no additional software installation is required. See these sections for information about the tasks required to use the Analytics Engine in integrated mode:

Installing the Network Director Analytics Engine in External Mode

The Analytics Engine in external mode runs on a separate, dedicated Analytics Engine server running CentOS. The following are the requirements for the Analytics Engine in external mode:

- The Analytics Engine server must run CentOS version 6.2, 64-bit.

- You can install the Analytics Engine directly on the CentOS server or on a virtual machine (VM).

  The server must have the following minimum system specifications:

  - 8 GB of RAM

  - 4 CPUs

  - 20 GB of hard disk space

  The following minimum system specifications are recommended:

  - 16 GB of RAM

  - 8 CPUs

  - 100 GB of hard disk space

- The Network Director server, the Analytics Engine server, and all devices to be monitored using the analytics feature must have network connectivity to each other, and have the following system time configurations:

  - Configured with the same time zone.

  - System clocks synchronized by using Network Time Protocol (NTP).

- The following network ports on the Analytics Engine server must be accessible to the Network Director server and all devices to be monitored using the analytics feature: 8080, 4242, 50005, 50006, 9160, 7000, and 9042.

The Analytics Engine is packaged as an RPM file. To install the Analytics Engine:

1. Prepare the CentOS 6.2 64-bit server. Note the server IP address.

2. Download the Analytics Engine RPM file from the Network Director software download page to the CentOS server.

    The RPM file filename has the following format: **ae-***release-identifier***.x86_64.rpm**—for example, **ae-1.6-R1.2.x86_64.rpm**.

3. Install the Analytics Engine on the server by entering the command **rpm –ivh** ***rpm-filename***, where *rpm-filename* is the name of the Analytics Engine RPM file.

4. You can verify the installation by entering these service status commands. An up status indicates successful installation:

    - **service cassandra status**

    - **service kairosdb status**

- service analytics-engine status

Configuring the Analytics Engine in Network Director

You must configure the Analytics Engine in Network Director to enable Network Director to monitor high-frequency statistics. To configure the Analytics Engine in Network Director:

1. Log in to Network Director.

2. Select **Preferences** from the drop-down menu next to the System button in the Network Director banner.

3. Select the **Monitoring** tab; then select **Analytics Engine Settings**.

4. In the **Server IP** field, enter the IP address of the Analytics Engine:

   - If you are running the Analytics Engine in integrated mode, enter the node IP address of the Junos Space server on which you want to run the Analytics Engine.

   - If you are running the Analytics Engine in external mode, enter the IP address of the Analytics Engine server.

5. Click **OK**.

Enabling High-Frequency Statistics on Devices

You need to enable high-frequency statistics on the devices you want to monitor. To enable high-frequency statistics on devices in Network Director:

1. Click **Deploy** in the Network Director banner to open Deploy mode.

2. Select the task **Configuration Deployment** > **Enable High Frequency Stats** in the Tasks pane.

   The Enable High Frequency Stats page opens. It contains a table listing the devices in inventory that support high-frequency statistics monitoring.

3. Select the check boxes next to the devices on which you want to enable high-frequency statistics.

4. Click **Deploy**.

Installing Cloud Analytics Engine

Cloud Analytics Engine uses network data analysis to improve the performance and availability of your applications. It supports data collection, analysis, correlation, and visualization, helping you better understand the behavior of workloads and applications across the physical and virtual infrastructure. Cloud Analytics Engine provides an aggregated and detailed level of visibility, tying applications and the network together, and an application-centric view of network status, improving your ability to quickly roll out new applications and troubleshoot problems.

Cloud Analytics Engine consists of the following software components:

- The Cloud Analytics Engine Junos OS component—This component is built into supported Junos OS releases and supports Cloud Analytics Engine. This component processes requests from Compute Agent to collect data. The collected data is sent to Compute Agent and is accessible on the device through **show** commands.

- Compute Agent—A required software component that is installed on a compute node. The Compute Agent works with the Cloud Analytics Engine Junos OS component to configure cloud analytics data collection on network devices and collect the requested data. The Compute Agent is controlled by either an API or by the Data Learning Engine component.

- Data Learning Engine—An optional software component that is installed on a compute node. It provides longer storage and additional processing of network analytics data. It also provides an API for integrating with Network Director to enable Network Director to configure analytics data collection and visualize network analytics data. Other applications can also use the API to integrate with Cloud Analytics Engine.

Network Director integrates with Data Learning Engine enabling you to configure, collect, and analyze cloud analytics data by using the Network Director user interface. Network Director uses the Data Learning Engine API to configure and collect cloud analytics data, and it can perform enhanced data processing, and provide more types of data.

Follow the instructions given in the Cloud Analytics Engine documentation available at Installing Cloud Analytics Engine page to install Cloud Analytics Engine.

For load sharing and optimum performance, you can have one or more Data Learning Engine components installed. After you install Data Learning Engine, you must enter the IP addresses of the servers that host each Data Learning Engine in the Preferences page in Network Director.

After completing the installation, you must integrate each Data Learning Engine with Network Director to enable Network Director to configure analytics data collection and visualize network analytics data.

To integrate a Data Learning Engine with Network Director:

1.
   Open the Preferences page in Network Director. Click in the Network Director banner and select **Preferences** as shown in Figure 2 on page 15.

Figure 2: Accessing the Preferences Page

2. In the Preferences page, open **Monitoring > Data Learning Engine Settings** sub-tab and enter the IP address and the port of the server or servers running Data Learning Engine.

    Click **Add Another** to add additional Data Learning Engine IP addresses.

3. Click **OK** to save the settings.

Uploading DMI Schemas

Each device type is described by a unique data model (DM) that contains all the configuration data for it. The DMI schema lists all the possible fields and attributes for a type of device. The later schemas describe the new features of recent device releases. It is important that you load all your device schemas into Junos Space Network Management Platform; otherwise only a default schema will be applied when you try to edit a device configuration by using the device configuration edit action in the Devices workspace.

In most installations, Junos Space automatically matches DMI schemas to device families. But there might be certain situations where your network uses a device for which Junos Space does not have the latest or supported schema available. In such instances, you must obtain and upload the requisite schema and set it as the default DMI schema for that device family. Set a default DMI schema for each device family to enable Junos Space to apply the appropriate schema to a device family.

If you cannot find the schema equivalent, use the latest schema from the main release or contact the Juniper Support. For example, for an EX4500 switch running Junos OS Release 13.2X51-D20, you must use the JUNOS 13.2X51-D20 schema. If this is not available, you can use the latest schema available from the JUNOS 13.2X51 releases. Use [xref target has no title] as a guideline for the fallback schema that you can obtain and upload in Junos Space before you start working with Network Director Release 2.5.

If you cannot find an appropriate schema for your device model from [xref target has no title], contact Juniper Support.

Table 1: DMI Schemas

Device	Name of the DMI Schema	Device Family
EX4300	JUNOS 14.1X53-D26	junos
EX9200	JUNOS 15.1R1	junos
EX4600	JUNOS 14.1X53-D26	junos-qfx

Table 1: DMI Schemas *(continued)*

Device	Name of the DMI Schema	Device Family
QFabric devices	JUNOS 14.1X53-D15	junos-qf
QFX3500 (non-ELS) QFX3600 (non-ELS)	JUNOS 12.3X50-D35	junos-qfx
QFX3500 with ELS (standalone and Virtual Chassis) QFX3600 with ELS (standalone and Virtual Chassis)	JUNOS 14.1X53-D26	junos-qfx
QFX5100-48S with ELS (standalone and Virtual Chassis) QFX5100-24Q with ELS (standalone and Virtual Chassis) QFX5100-96S with ELS (standalone and Virtual Chassis)	JUNOS 14.1X53-D26	junos-qfx
QFX5100 switches with the following product SKUs: QFX5100-48S-3AFI QFX5100-24Q-3AFI QFX5100-24Q-3AFO QFX5100-24Q-D-3AFI QFX5100-24Q-D-3AFO	JUNOS 14.1X53-D26	junos-qfx
QFX5100 switches with the following product SKUs: QFX5100-48T-AFI QFX5100-48T-AFO QFX5100-48T-DC-AFI QFX5100-48T-DC-AFO	JUNOS 14.1X53-D26	junos-qfx
MX Series Routers in LAN mode MX240 MX480 MX960 Series routers	JUNOS 15.1R1	junos

To install or update a DMI schema on Junos Space:

1. From the Network Application Platform, navigate to **Administration > Manage DMI Schemas > Update Schema**.

   The Update Schema page appears.

   To add or update a DMI schema, you must have the **.tgz** archive files containing the schema on the machine running the Junos Space GUI. There are several ways of acquiring such files. You can:

   - Download files from Juniper's SVN Repository.

   - Obtain files from Juniper Support staff.

   - Create your own files.

   For detailed steps on acquiring and uploading the schema files, see Junos Space Documentation or Managing DMI Schemas Overview.

2. After uploading the schema, select the schema and click **Install**.

   The Manage DMI Schemas inventory landing page appears, displaying the newly installed schema. The Manage DMI Schemas page displays data in a table that has the following columns:

   - Device Family

   - OS Version

   - Device Series

   - State—Whether default or not. An empty cell in this column means that the DMI schema in that row is not the default.

     In the thumbnail view, this information is displayed on each thumbnail.

3. In the tabular view, select the row that contains the appropriate combination of device family, OS version, and device series, and mouse over the **Actions** drawer to select **Set Default Schema**.

   In the thumbnail view, select the appropriate thumbnail and perform the same action.

   The Set Default DMI Schema dialog box opens, displaying the DMI schema name, device family, and OS version.

4. Click **Set Default**.

   If any other schema was previously the default, in the tabular view, the cell in the State column appears empty, and the word *Default* appears in the State column for the selected schema. In the thumbnail view, the default status is indicated by an orange-colored asterisk on the icon for a DMI schema, and the word *Default* below the OS version.

Preparing Devices for Management by Network Director

To discover and manage devices, Network Director requires the following minimum device configuration as a prerequisite for installation on a device. Ensure that the device:

- Has a static management IP address. The address can be in-band or out-of-band, but must be reachable from the Junos Space server.

- Is enabled for SSH v2. On wireless LAN controllers, SSH is enabled by default. However, on EX Series switches you need to enable SSH. Issue the **set system services ssh protocol-version v2** command to enable SSH v2 on EX Series switches.

- Has a user ID with the superuser class configured. Junos Space, and Network Director use this user ID to authenticate the SSH connection with the device.

- Is enabled for SNMP with the appropriate read-only V1, V2, and V3 credentials created. You do not need to configure SNMP trap receivers; Network Director configures traps as a deployment task.

In addition, the following protocol ports must be open for Network Director communication:

- Port 22 for SSH connections. If you have changed the SSH port to a port other than port 22 on your Network Management Platform, you must change the SSH ports on your managed devices to the port that the Network Management Platform is using.

- Port 443 for virtualization and RingMaster import support. Use port 443 for outbound traffic to vCenter servers.

> **NOTE:** 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.

- Port 10162 for SNMP traps. Network Director receives traps from managed devices on this port. (After you install Network Director, use Network Director to configure SNMP on your devices to send traps to Network Director on this port.)

- Port 8889 for the management of wireless LAN controllers.

- Port 21 (TCP) and port 69 (UDP) for uploading the software image and configuration file to the FTP server.

- Ports 8774, 9696, 9292, 8777, 35357, and 8776 for accessing OpenStack and VMware NSX APIs.

You can verify whether a port is open by logging in to the Junos Space CLI and using the **nmap** command. For example, to determine whether port 8889 is open on a controller, issue this command:

root@space# nmap <*IP address of controller*> -p 8889

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.

Figure 3: Select Build Mode and Discover Devices Task
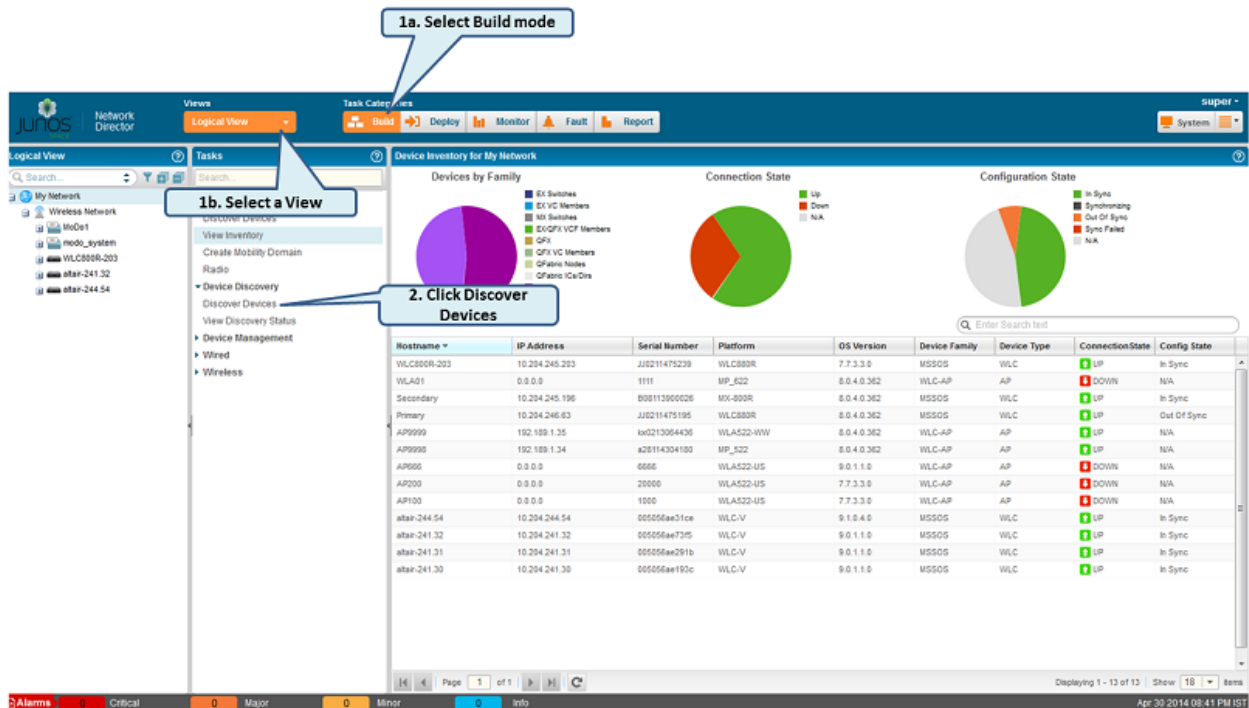
3. (Optional) Type a name for the discovery job. The default name is ND Discovery.

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.

Figure 4: Start Discover Devices Wizard
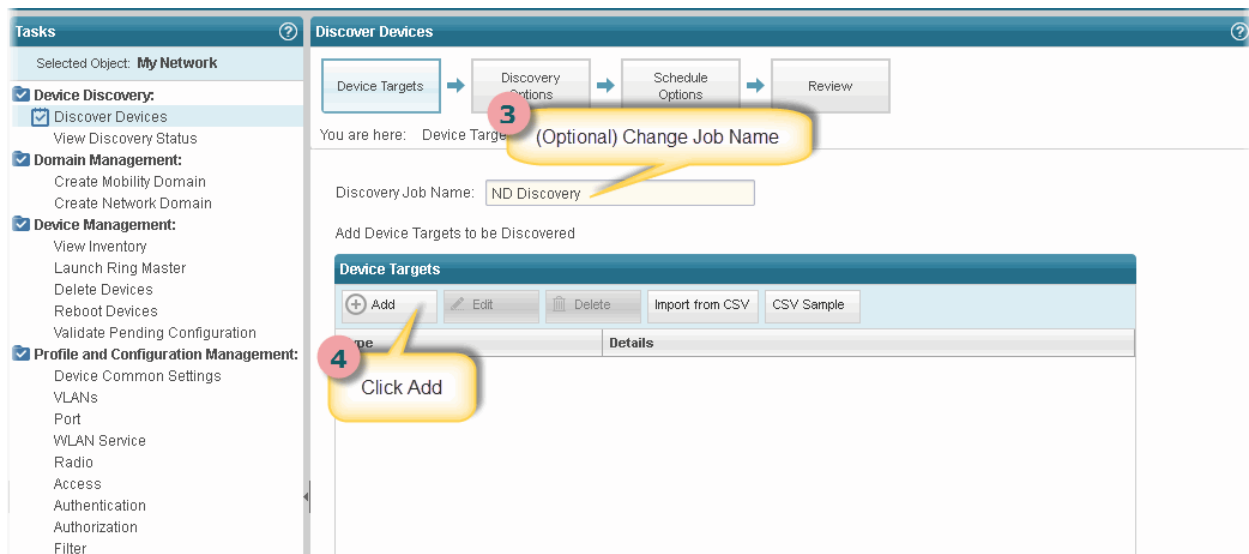
5. Provide the initial or the lowest IP address value and the ending or highest IP address value for the range and click **Add**. You can have up to 1024 devices in a range. After you click Add, the address range is listed in the Device Targets window.

Figure 5: Specify the IP Range
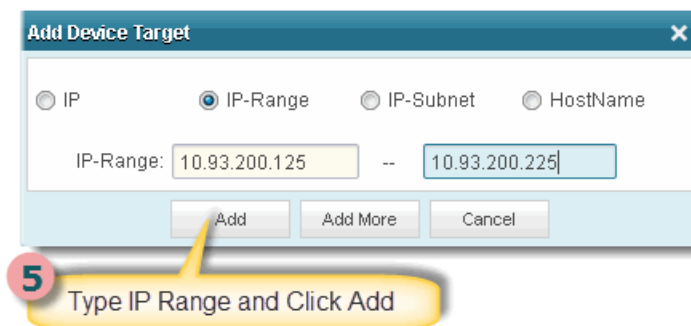
6. Click **Next** or click **Discovery Options** to proceed to specify the device credentials and method of discovery.

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.

   If you select SNMP, the Add SNMP Settings dialog box is displayed. In this example, because we run SNMP version 2, 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.

Figure 6: Provide Device Credentials and Discovery Method

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.

Figure 7: Review Discovery Settings

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.

Figure 8: View Discovery Results

Related Documentation

- *Troubleshooting Device Discovery Error Messages*

Next Steps

After your devices are up and synchronized, much of the function in Network Director is automatically enabled. However, there are a few additional tasks that you will need to perform to use all the features of Network Director. We suggest that you explore:

- Set up a Location View

  Location View is one of seven different views, or perspectives, in your network. In Location View, you can manage devices based on a site. Here you define the buildings, floors, wiring closets, and outdoor areas. You can upload floor maps for easy reference and assign devices to a specific spot.

  To set up a Location View:

  1. Click **Build** in the Network Director banner.

  2. Select **Location View** in the View pane to the far left of the screen.

  3. Click **Setup Locations** in the Tasks pane to start setting up your location, buildings, floors, racks, wiring closets, and outdoor areas.

- Enable Trap Forwarding and Alarms for Fault Management

  A key component of Network Director is the feature to diagnose problems with precision and ease. Network Director correlates multiple traps from the same device to a single alarm.

  You must complete device discovery and the devices must be up before you can enable trap forwarding. Traps are not enabled by default; you need to enable them after device discovery.

  1. Use **Set SNMP Trap Configuration** in the Tasks pane of Deploy mode to configure your device to send SNMP traps to Network Director.

  2. Review the list of alarms in Preferences, located in the Network Director banner. All alarms are enabled by default, but you might want to disable those alarms that are not pertinent to your installation. You can also change the severity of an alarm by using Preferences.

- Set up users

  After you install Network Director, there is only one username defined: *super* with the default password, *juniper123*.

  You have the ability to set up users with different Network Director privileges. New Network Director users are set up in Junos Space and follow the roles and privileges as defined in Junos Space. For a complete discussion on how to properly set up users, see *Understanding Network Director User Administration*.

- Learn what you can do with Network Director

  There are two ways you can become familiar with the functions and features of Network Director:

- Read *Introduction to Junos Space Network Director*. This short guide highlights the primary features of Network Director.

- Use the extensive help system that guides you through Network Director. Clicking the main Help icon provides a top-down view into the help system; clicking a Help icon on a pane or window provides context-sensitive information. Use the help system to familiarize yourself with Network Director and the different modes and panes in the interface.

Network Director API Setup Sample Files

After you install the Network Director API software, the only NaaS service that is available for use is the service for importing the physical network topology of the NaaS domain. Before you can use the full set of NaaS service resources with the API, you must initialize the NaaS service and import static configurations to your managed devices.

Before you import the NaaS domain physical topology to devices, prepare a topology file.

This topic provides the following sample file:

- Sample Physical Topology File on page 26

Sample Physical Topology File

The following output shows a sample physical topology file in XML format.

```xml
<NaasDomains>
  <NaasDomain name="Naas-Domain-Name">
    <topology>
      <systems>
        <system name="ex4-host-name" mgmtIp="192.168.1.0" userId="root" password="SecretPassword">
          <capabilities>
            <capability name="SWITCHING" />
          </capabilities>
          <revenueport_ifds>
            <revenueport_ifd name="ge-0/0/3"/>
            <revenueport_ifd name="ge-0/0/22"/>
            <revenueport_ifd name="ge-0/0/23"/>
            <revenueport_ifd name="ge-0/0/24"/>
          </revenueport_ifds>
        </system>
        <system name="srx-host-name" mgmtIp="10.94.45.185" userId="root" password="password">
          <capabilities>
            <capability name="SECURITY" />
          </capabilities>
          <revenueport_ifds>
            <revenueport_ifd name="ge-0/0/1"/>
            <revenueport_ifd name="ge-0/0/2"/>
            <revenueport_ifd name="ge-1/0/3"/>
            <revenueport_ifd name="ge-0/0/4"/>
            <revenueport_ifd name="ge-0/0/5"/>
            <revenueport_ifd name="ge-0/0/6"/>
          </revenueport_ifds>
        </system>
      </systems>
      <linked_interfaces>
```

```
    <ifd name="ge-1/0/3">
      <peer name="ge-0/0/23">
        <hostedOn name="ex4-host-name"/>
      </peer>
      <hostedOn name="srx-host-name"/>
    </ifd>
      </linked_interfaces>
    </topology>
  </NaasDomain>
</NaasDomains>
```

Table 2 on page 27 describes the NaaS domain physical topology information that you must provide in the topology file.

Table 2: Physical Topology Input Fields

Field Name	Description
NaasDomain name	Name of the NaaS domain in the topology. Only one NaaS domain is supported.
NaaS Domain Components	
system name	System name of each device managed by the NaaS domain. For each system name, provide the following system information: • Management IP address (mgmtIp) • User ID (userId) of the system administrator • Password (password) for the user ID NOTE: Only one device with switching capability is supported in each NaaS domain.
System Components	
capability name	Capability you enable for each system (managed device). Valid values are: • ROUTING • SECURITY • SWITCHING NOTE: Only one device with switching capability is supported in each NaaS domain.
revenueport_ifd name	Interface name that identifies a revenue port in a system; for example, ge-0/0/3. Revenue ports are attachment points that connect to physical servers.
Linked Interfaces Components (Optional for topologies with a single device)	
ifd name	Name of an interface that is connected to a peer interface. An ifd name must be paired with a peer name.
peer name	Name of the peer interface.

Table 2: Physical Topology Input Fields *(continued)*

Field Name	Description
hostedOn name	Hostname of an interface. Each linked interface must have a hostname.

Related Documentation

- *Overview of Network Director API*
- *Setting Up the Network Director API*
- *Sample API Scripts Overview*