JUNIPER NETWORKS | Engineering Simplicity

Junos Space Network Management Platform

Getting Started Guide

Published
2022-06-16

RELEASE
21.3

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

Junos Space Network Management Platform Getting Started Guide
21.3

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 This Guide

Use this guide to understand the architecture and deployment of a Junos Space fabric. It also includes procedures for uninstalling, upgrading, and installing Junos Space applications, and upgrading Junos Space Platform. You can also find procedures for managing devices, such as discovering devices, viewing device inventory, upgrading device images, managing device configurations, and so on.

CHAPTER 1

Junos Space Fabric Deployment

Junos Space Fabric Architecture

To support the rapid growth in network size, Junos Space is designed to be highly scalable. You can cluster multiple Junos Space appliances to create a single management fabric, which is accessible from a single virtual IP (VIP) address.

All graphical user interface (GUI) and northbound interface (NBI) clients use the Junos Space VIP address to connect to the Junos Space fabric. The fabric incorporates a front-end load balancer that distributes client sessions across all the active Junos Space nodes within the fabric. You can increase or decrease the fabric by simply adding or deleting nodes to or from the Junos Space Network Management Platform user interface, and the Junos Space system automatically starts applications and services on the active nodes. Each node in the cluster is fully utilized and all nodes work together to provide automated resource management and service availability.

A Junos Space fabric architecture comprising multiple appliances eliminates any single point of failure. When a node in the fabric goes down, all client sessions and device connections currently served by that node are automatically migrated to the active nodes in the fabric without any user-initiated action.

RELATED DOCUMENTATION

Junos Space Fabric Deployment Overview | 2

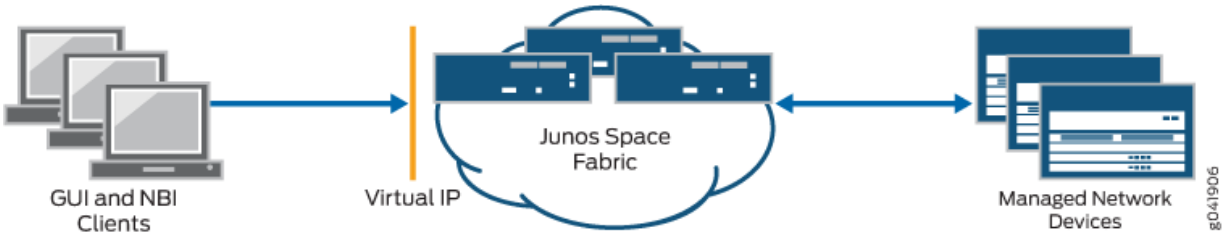
Junos Space Fabric Deployment Overview

IN THIS SECTION

You can install and deploy Junos Space Hardware Appliances JA2500), Junos Space Virtual Appliances, or both to form a fabric. Each appliance in the fabric is called a *node*. All nodes in the fabric work together as a cluster of Junos Space instances running in active-active configuration (that is, all nodes are active in the cluster).

Figure 1 on page 3 displays how a Junos Space fabric employs a software load balancer to distribute HTTP sessions across the nodes to ensure that the load presented by the Junos Space Network Management Platform user interface and NBI clients is equally distributed within the fabric.

Figure 1: Clients Using a Single Virtual IP Address to Access the Junos Space Fabric



A Junos Space fabric of appliances provides scalability and ensures high availability of your management platform. The fabric provides an N+1 redundancy solution where the failure of a single node in the fabric does not affect the functioning of the fabric. When a node in the fabric fails, the sessions of the clients accessing Junos Space from the user interface automatically migrate away from the failed node. Similarly, managed devices that were connected to the failed node are automatically reconnected with another functioning node in the fabric.

Deploying a Junos Space Hardware Appliance

When you power on the Junos Space Hardware Appliance and log in to the CLI console, you can view a menu-driven command-line interface to specify the initial configuration of the appliance.

You need to specify the following parameters:

- IP address and subnet mask for the “eth0” interface
- Virtual IP address (when you configure the first node in the cluster) to access the Junos Space user interface from Web browsers. The IP address should be in the same subnet as the IP address assigned to the “eth0” interface.
- IP address of the default gateway
- IP address of the name server

- IP address and subnet mask for the “eth3” interface if you choose to manage devices on a different Ethernet interface (see Figure 3 on page 7).
- Whether the appliance will be added to an existing cluster. Choose “n” to add the first node to a new cluster and choose “y” to add subsequent nodes to the cluster.
- NTP server settings with which to synchronize the appliance’s time
- Maintenance mode user ID and password

> **NOTE**: Ensure that you remember the Maintenance mode user ID and password. These details are required when you upgrade software and restore databases.

Refer to the *JA2500 Junos Space Appliance Quick Start Guide* for detailed instructions on how to configure the hardware appliance during initial deployment.

Deploying a Junos Space Virtual Appliance

The Junos Space Virtual Appliance is stored in the open virtual appliance (OVA) format and is packaged as an ***.ova** file, which is a single folder that contains all the files of the Junos Space Virtual Appliance. OVA is not a bootable format and you must deploy each Junos Space Virtual Appliance to a hosted ESX or ESXi server before you can run the Junos Space Virtual Appliance.

You can deploy a Junos Space Virtual Appliance on a VMware ESX server version 4.0 or later or VMware ESXi server version 4.0 or later. After the Junos Space Virtual Appliance is deployed, you can use the VMware vSphere client that is connected to the VMware ESX (or VMware ESXi) server to configure the Junos Space Virtual Appliance. You can deploy Junos Space Virtual Appliance 14.1R2.0 and later on qemu-kvm Release 0.12.1.2-2/448.el6. You must deploy and configure the Junos Space Virtual Appliance on a KVM server by using the Virtual Machine Manager (VMM) client.

The CPU, RAM, and disk space provided by the VMware ESX server or KVM server must meet or exceed the documented CPU, RAM, and disk space requirements for deploying a Junos Space Virtual Appliance. In addition, we recommend that, for a multinode fabric, you deploy the first and second virtual appliances on separate servers to ensure failover support.

> **NOTE**: Starting from VMware ESX server 6.5 and above, 32GB of RAM, 4core CPU and 500GB of disk space gets created by default to execute or install an OVA image.

The distributed Junos Space Virtual Appliance files are created with 135 GB of disk space. If you create a multinode cluster, ensure that the first and second nodes that you deploy should contain the same

amount of disk space. When the disk resources are used beyond 80% capacity, add sufficient disk space (more than 10 GB) to the disk partitions.

When you log in to the console of the VMware vSphere client or VMM client, you need to specify the same parameters used to deploy a hardware appliance. Refer to the *Junos Space Virtual Appliance Deployment and Configuration Guide* for detailed instructions on how to configure the virtual appliance during initial deployment.

Basic Requirements for a Fabric Deployment

When you deploy multiple appliances to create a Junos Space fabric, each appliance in the fabric uses the eth0 interface for all internode communication within the fabric. On each appliance, you can choose to use a separate interface (eth3) for all communication between the appliance and managed devices, as shown in Figure 3 on page 7.

The following are required when you deploy a Junos Space fabric:

- You must be able to ping the default gateway IP address, or else the fabric will not form correctly.
- The IP addresses assigned to the eth0 interface on the first two appliances in the fabric must be in the same subnet.
- The virtual IP address configured on the first appliance in the fabric must be in the same subnet as the eth0 interface on the first two appliances.
- Multicast packets must be routable among all nodes because JBoss cluster-member discovery uses multicast routing.
- If you are deploying a fabric of virtual appliances, we recommend that the first and second appliances added to the fabric be hosted on a separate VMware ESX or ESXI server to ensure failover support.
- All appliances in the fabric must use the same external NTP source to ensure consistent time setting across all appliances in the fabric You must specify the NTP source on each appliance before adding the appliance to the fabric.
- All nodes in the fabric are running the same version of the software.

Configuring Network Connectivity for a Junos Space Fabric

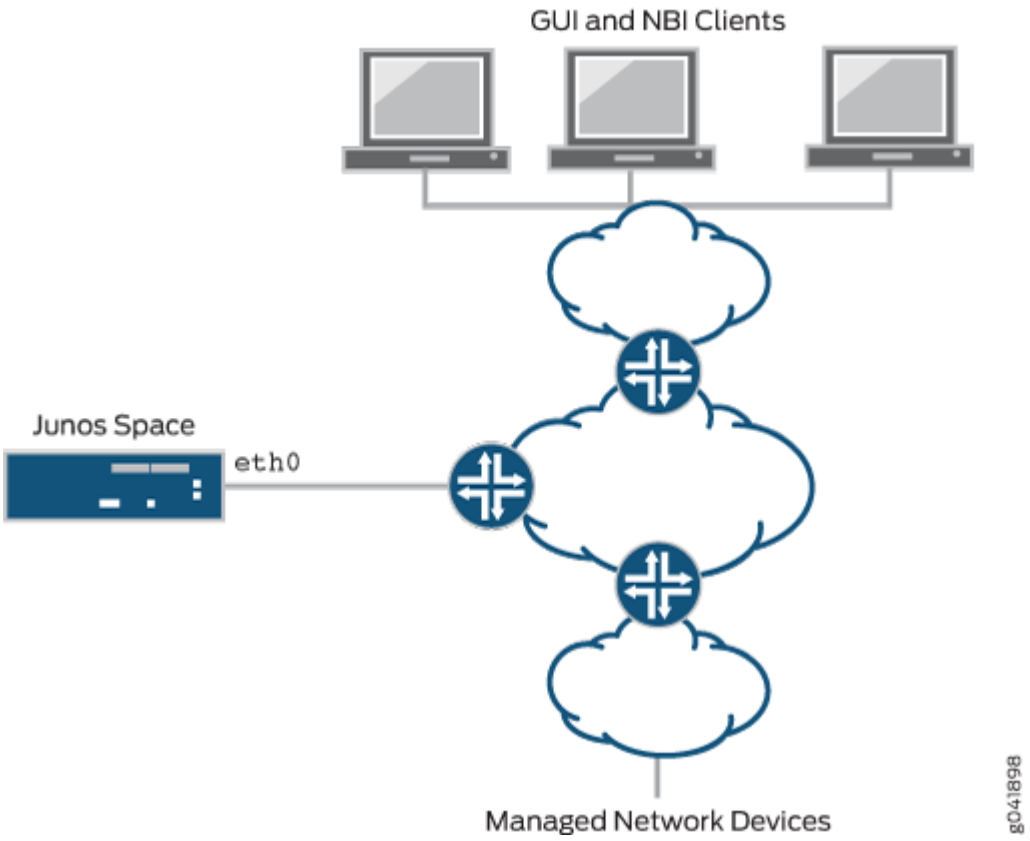
A Junos Space appliance (hardware or virtual) has four RJ45 10/100/1000 Ethernet interfaces that are named eth0, eth1, eth2, and eth3. When deploying the appliance, you need to ensure that it has IP connectivity with the following:

- Devices in your managed network
- Desktops, laptops, and workstations from which Junos Space users access the Junos Space user interface as well as external systems hosting NBI clients
- Other appliances that form a Junos Space fabric along with this appliance

Junos Space allows you to use two of the four Ethernet interfaces: eth0 and eth3. The other two Ethernet interfaces are reserved for future use. You can choose one of the following two options for configuring interfaces for IP connectivity:

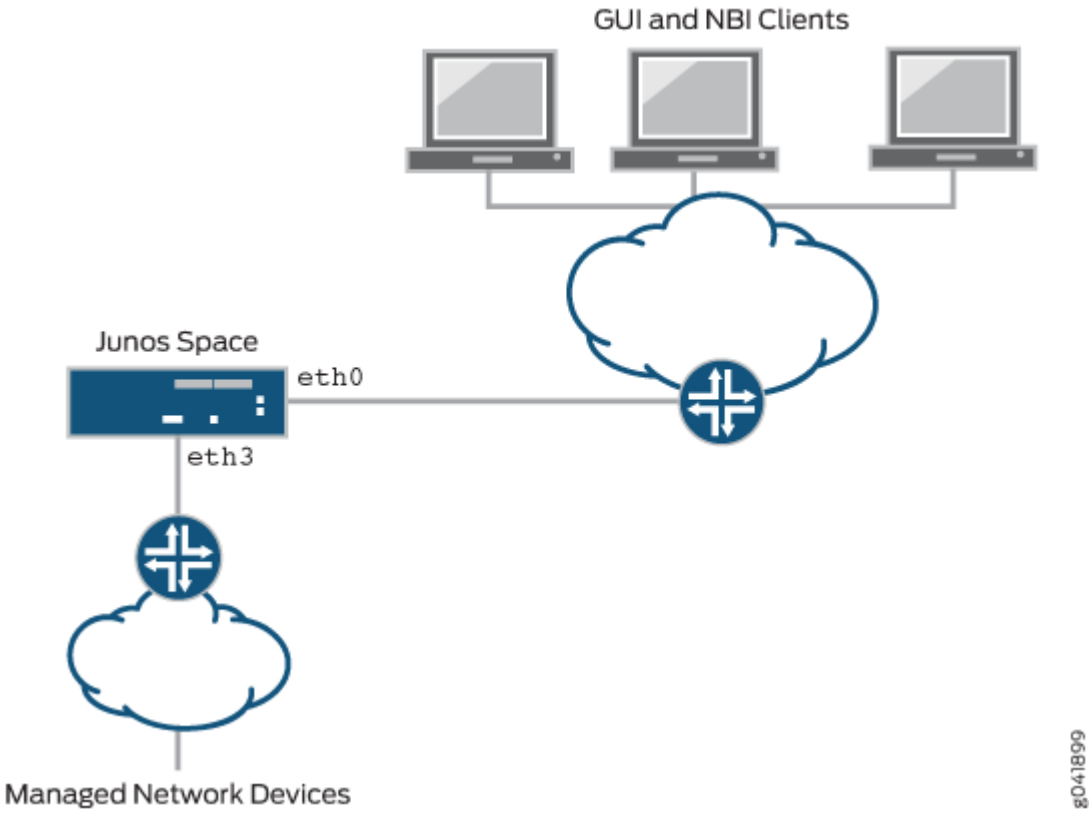
- Use the eth0 interface for all network connectivity of the appliance, as shown in Figure 2 on page 6.

Figure 2: Using a Single Ethernet Interface for All IP Connectivity



- Use the eth0 interface for network connectivity with Junos Space user interface clients and other appliances in the same fabric, and use the eth3 interface for network connectivity with managed devices, as shown in Figure 3 on page 7.

Figure 3: Using Two Interfaces for IP Connectivity



Adding Nodes to a Junos Space Fabric

You must be assigned the System Administrator user role to be able to add nodes to a Junos Space fabric. You add nodes to a Junos Space fabric from the **Add Fabric Node** page (**Network Management Platform > Administration > Fabric > Add Fabric Node**). To add a node to a fabric, you specify the IP address assigned to the eth0 interface of the new node, a name for the new node, and (optionally) a scheduled date and time to add the node to the fabric. Junos Space software automatically handles all necessary configuration changes to add the node to the fabric. After the new node is added to the fabric, you can monitor the status of the node from the **Fabric** page (**Network Management Platform > Administration > Fabric**).

For complete information about adding nodes to a fabric, see the *Adding a Node to an Existing Junos Space Fabric* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

RELATED DOCUMENTATION

Junos Space Fabric Architecture | 2

Installing and Upgrading Junos Space Software Overview | 10

2

CHAPTER

Junos Space System Administration

Installing and Upgrading Junos Space Software Overview

IN THIS SECTION

The following sections describe the primary software administration tasks for the Junos Space Network Management Platform and Junos Space applications:

CAUTION: Do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, the installation or upgrade fails.

NOTE: Juniper Networks devices require a license to activate the feature. To understand more about Junos Space Network Management Platform Licenses, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

Installing Junos Space Applications

Before installing an application, verify that the application is compatible with the Junos Space Network Management Platform. For more information about application compatibility, see the Knowledge Base article KB27572 at https://kb.juniper.net/InfoCenter/index?page=content&id=KB27572.

You can upload an application image file to Junos Space from the **Add Application** page (**Administration > Applications > Add Application**). You can upload an application image file by using HTTP (**Upload via**

HTTP) option or Secure Copy Protocol (SCP) (**Upload via SCP**) option. We recommend that you upload the file by using SCP, which initiates a direct transfer from an SCP server to Junos Space and is performed as a back-end job. If you choose to upload the file using SCP, you must first make the image file available on an SCP server that Junos Space can access. You must also provide the IP address of the SCP server and the login credentials needed to access this SCP server. The main advantage of using SCP is that your user interface is not blocked while the file transfer is in progress, and you can monitor the progress of the file transfer from the **Jobs** workspace.

> **NOTE**: A Junos Space node can also be used as an SCP server. To do this, copy the application image file (using SCP or SSH FTP [SFTP]) to the **/tmp/** directory on the Junos Space node, and in the **Upload Software via SCP** dialog box specify the credentials (username and password), the IP address of the Junos Space node, the CLI credentials, and the file path for the software image.

After the image file for the application is uploaded successfully, you can view the application from the **Add Application** page. You can then select the application file and click the **Install** button to install the application. The application installation process does not cause any downtime for the Junos Space Network Management Platform or any applications installed on Junos Space. Junos Space Network Management Platform ensures that the application is installed on all nodes in the Junos Space fabric and access to the application is load balanced across all nodes in the Junos Space fabric.

For more information about installing Junos Space applications, see the *Managing Junos Space Applications Overview* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Upgrading Junos Space Applications

You can easily upgrade a Junos Space application from the Junos Space Platform UI. You must download the image file for the new version of the application, navigate to the **Applications** page (**Administration > Applications**), right-click the application that you want to upgrade, and select **Upgrade Application** to upload the image file into Junos Space through HTTP or SCP. We recommend that you use the SCP option, which initiates a direct transfer from an SCP server to Junos Space. After the image file is uploaded, select the uploaded file and click the **Upgrade** button to start the upgrade process. If you perform the upgrade by using SCP, then the upgrade process is executed as a back-end job by the Junos Space Network Management Platform, and you can monitor the progress of the upgrade from the **Jobs** workspace. An application upgrade does not cause downtime for the Junos Space Network Management Platform or other applications that are hosted by Junos Space.

For more information about upgrading Junos Space applications, see the *Managing Junos Space Applications Overview* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Upgrading Junos Space Network Management Platform

Juniper Networks typically produces two major releases of the Junos Space Network Management Platform per year. In addition, one or more patch releases might accompany each major release. You can upgrade to a newer Junos Space Platform release by performing a few simple steps from the user interface in your current Junos Space Platform.

NOTE: If you are upgrading to Junos Space Platform Release 16.1R1 or 16.1R2, follow the procedure outlined in the topic *Upgrading to Junos Space Network Management Platform Release 16.1R1* in the Workspaces User Guide.

WARNING: Upgrading to a new Junos Space Network Management Platform version might disable functionality and the ability to use the installed Junos Space applications. Before you upgrade the Junos Space Network Management Platform, take inventory of the applications installed. If Junos Space Network Management Platform is upgraded and a compatible application is not available, the installed application is deactivated and cannot be used until a compatible application has been released.

If you are upgrading Junos Space Platform to releases other than Junos Space Platform Release 16.1R1, the workflow for performing the upgrade is similar to that of installing an application. After you download the required image file, (**.img** extension) from the Juniper Networks software download site, navigate to the **Applications** page (**Administration > Applications**), right-click the image file, and select **Upgrade Platform** to upload the image file into Junos Space through HTTP or SCP. We recommend that you use the SCP option, which initiates a direct transfer from an SCP server to Junos Space and is performed as a back-end job. If you choose the SCP option, you must first make the image file available on an SCP server that Junos Space can access. After the image file is uploaded, select the uploaded file, and click the **Upgrade** button to start the upgrade process. The Network Management Platform upgrade forces the system into Maintenance mode, which requires that you enter the Maintenance mode username and password to proceed with the upgrade.

During the Junos Space Network Management Platform upgrade process, all the data in the Junos Space database is migrated to the new schema that is part of the new Junos Space release. The upgrade process also seamlessly upgrades all nodes in the fabric. The upgrade process requires a restart of JBoss application servers on all nodes and might also require a reboot of all the nodes if the OS packages are also upgraded. The time required for the upgrade depends on a number of factors, including the amount of data being migrated, the number of nodes in the fabric, and the number of third-party components upgraded. You should expect an average downtime of 30 to 45 minutes for upgrade of a single-node fabric, and approximately 45 to 60 minutes for upgrade of a two-node fabric.

NOTE: You can use this workflow to upgrade to Release 18.1 from Release 17.2 or Release 17.1. If you are upgrading to Release 18.1 from a release earlier than 16.1, you must first upgrade the installation to Release 16.1 and then, upgrade to Release 17.1 or Release 17.2. You must perform multistep upgrades if a direct upgrade is not supported between the version from which you want to upgrade and the version to which you want to upgrade. For detailed information about the releases from which Junos Space Platform can be upgraded, see the *Junos Space Network Management Platform Release Notes*.

Before you upgrade Junos Space Platform to Release 18.1, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see *Synchronizing Time Across Junos Space Nodes*.

For more information about upgrading the Junos Space Network Management Platform, see the *Upgrading Junos Space Network Management Platform Overview* topic in the *Junos Space Network Management Platform* Workspaces User Guide.

Uninstalling Junos Space Applications

To uninstall a Junos Space application, navigate to the **Applications** page (**Administration > Applications**), right-click the application that you want to uninstall, and select **Uninstall Application**. You are prompted to confirm the uninstallation process. Upon confirmation, the uninstallation process for the application is executed as a back-end job by Junos Space. You can monitor the progress of the job from the **Job Management** page (**Jobs > Job Management**). The uninstallation process does not cause downtime for Junos Space Network Management Platform or other applications hosted by Junos Space Network Management Platform.

For more information about uninstalling Junos Space applications, see the *Uninstalling a Junos Space Application* topic in the *Junos Space Network Management Platform* Workspaces User Guide).

RELATED DOCUMENTATION

Junos Space License Installation Overview

Junos Space Applications Supported on the Junos Space Platform | 14

Configuring User Access Controls Overview | 17

Junos Space Applications Supported on the Junos Space Platform

A number of high-level applications are available for Junos Space Network Management Platform. You can install these applications to simplify network operations, scale services, automate support, and open the network to new business opportunities.

The Junos Space Network Management Platform is a multitenant platform that enables you to install hot-pluggable applications. Junos Space automatically deploys the installed applications across the fabric. You can install, upgrade, and remove applications without disrupting or causing any downtime for the Junos Space Network Management Platform or other hosted applications.

The following applications are currently available for Junos Space Network Management Platform:

- Junos Space Log Director–Enables log collection across SRX Series Services Gateways and enables log visualization
- Junos Space Network Director–Enables unified management of Juniper Networks EX Series Ethernet Switches, EX Series Ethernet switches with ELS support, QFX Series switches, QFabric, wireless LAN devices, and VMware vCenter devices in your network
- Junos Space Security Director –Allows you to secure your network by creating and publishing firewall policies, IPsec VPNs, network address translation (NAT) policies, intrusion prevention system (IPS) policies, and application firewalls
- Junos Space Services Activation Director–Collection of the following applications that facilitate automated design and provisioning of Layer 2 VPN and Layer 3 VPN services, configuration of QoS profiles, validation and monitoring of service performance, and management of synchronization:
  - Network Activate
  - Junos Space OAM Insight
  - Junos Space QoS Design
  - Junos Space Transport Activate
  - Junos Space Sync Design
- Junos Space Service Automation–End-to-end solution designed to streamline operations and enable proactive network management for Junos OS devices. The Service Automation solution consists of the following:
  - Junos Space Service Now

  - Junos Space Service Insight
  - Advanced Insight Scripts (AI-Scripts)
- Junos Space Virtual Director–Enables the provisioning, bootstrapping, monitoring, and lifecycle management of a variety of Juniper virtual appliances and related virtual security solutions

NOTE: For information about the Junos Space applications supported for a specific version of the Junos Space Network Management Platform, see the Knowledge Base article KB27572 at https://kb.juniper.net/InfoCenter/index?page=content&id=KB27572.

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 10

DMI Schema Overview

Each device type is described by a unique data model that contains all the configuration data for that device. The schemas for this data model list all the possible fields and attributes for a type of device. The newer schemas describe the new features associated with recent device releases.

Junos Space Network Management Platform provides support for managing devices based on Device Management Interface (DMI) schema.

You must load all your device schemas into Junos Space Network Management Platform; otherwise, only a default schema is applied when you try to edit a device configuration using the device configuration edit action in the Devices workspace (as described in *Modifying the Configuration on the Device* in the *Junos Space Network Management Platform* Workspaces User Guide).

If the Junos Space Network Management Platform contains exactly the right schema for each of your devices, you can access all the configuration options specific to each device. You can add or update schemas for all Junos Space devices from the Administration workspace (**Administration > DMI Schemas**) workspace. You can use this workspace to check whether a schema for a device is missing. On the Manage DMI Schemas page, in tabular view, the DMI Schema column displays *Need Import* if the Junos OS schema for that particular device OS is not bundled with the Junos Space Network Management Platform. Then you need to download the schema from the Juniper Schema Repository.

For complete information about managing DMI schema , see the *DMI Schema Management Overview* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

RELATED DOCUMENTATION

Device Management in Junos Space Platform | 27

Backing Up the Junos Space Platform Database

You must back up the Junos Space database regularly so that you are able to roll back the system data to a previously known point. You can create a backup schedule on the **Database Backup and Restore** page in the **Administration** workspace (**Network Management Platform > Administration > Database Backup and Restore**). You can store the backup file on the local file system of the Junos Space appliance, or on a remote server by using the Secure Copy Protocol (SCP).

NOTE: We recommend that you back up files on a remote server because this ensures that the backup files are available even if an error occurs on the appliance. In addition, if you back up files remotely instead of locally, you ensure optimal use of the disk space on the Junos Space appliance.

To perform remote backups, you must set up a remote server that can be accessed through the SCP and that has its IP address and credentials available. We recommend that you have a separate partition on this server to store Junos Space backups and that you provide the full path of this partition in the Junos Space user interface when you set up the backup schedule. You can also specify the start date and time for the first backup, the recurrence interval required (hourly, daily, weekly, monthly, or yearly), and the date and time of the last backup (if required). In most cases, we recommend that you back up the database daily. You can customize the backup frequency based on the needs of your organization and the amount of change that occurs in the network. In addition, you can schedule backups to run automatically when the system usage is low. Creating a backup schedule ensures that database backups occur at the scheduled time and at the scheduled recurrence intervals. You can also perform database backups on demand from the **Database Backup and Restore** page, in the **Administration** workspace (**Network Management Platform > Administration > Database Backup and Restore**), by clearing the check boxes that control the time of occurrence and recurrence intervals.

Whether scheduled or performed on demand, each successful backup generates an entry that is available on the **Database Backup and Restore** page. You can select the database backup entry and select the **Restore From Remote File** action to restore the system data to the selected backup.

NOTE: Performing a database restore action causes a downtime in your Junos Space fabric, which goes into Maintenance mode to restore the database from the chosen backup and then waits for the application servers to be restarted.

For complete information about performing backup and restore operations for the Junos Space Network Management Platform, see the *Backing Up and Restoring the Database Overview* and *Backing Up the Junos Space Network Management Platform Database* topics (in the *Junos Space Network Management Platform* Workspaces User Guide).

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 10

Junos Space Applications Supported on the Junos Space Platform | 14

Configuring User Access Controls Overview

IN THIS SECTION

Junos Space Network Management Platform provides a robust user access control mechanism system that you use to enforce appropriate access policies on the Junos Space system through your Junos Space administrators. In Junos Space, administrators can serve different functional roles. A CLI administrator installs and configures Junos Space appliances. A Maintenance-mode administrator performs system-level tasks, such as troubleshooting and database restoration operations. After the

appliances are installed and configured, you can create users and assign roles that allow these users to access the Junos Space Platform workspaces and manage the applications, users, devices, services, customers, and so forth.

Table 1 on page 18 shows the Junos Space administrators and the tasks that can be performed.

Table 1: Junos Space Administrators

Junos Space Administrator Function	Description	Tasks

CLI administrator	An administrator responsible for setting up and managing system settings for Junos Space appliances from the serial console
	
	The CLI administrator name is *admin*.
	
	The CLI administrator password can be changed from the console system settings menu.
		• Install and configure basic settings for Junos Space appliances.
		
		• Change network and system settings for appliances, for example:
		
		  • Change the CLI administrator password.
		
		  • Modify routing parameters.
		
		  • Modify DNS server settings.
		
		  • Change time zone and NTP server settings.
		
		  • Expand the VM drive size (Junos Space Virtual Appliances only).
		
		  • Retrieve log files for troubleshooting.

Maintenance-mode administrator	An administrator responsible for performing system-level maintenance on Junos Space Network Management Platform The Maintenance-mode administrator name is *maintenance*. The Maintenance-mode password is configured from the serial console when you first configure a Junos Space appliance.	• Restore Junos Space Network Management Platform to its previous state by using a database backup file. • Shut down Junos Space nodes by entering Maintenance mode. • Retrieve log files for troubleshooting. • Exit Maintenance mode and explicitly start up the Junos Space system.
Junos Space user interface users	A Junos Space user that is assigned one or more predefined roles. Each role assigned to a user provides specific access and management privileges on the objects (applications, devices, users, jobs, services, and customers) available from a workspace in the Junos Space user interface.	For more information about the predefined roles that can be assigned to a Junos Space user, see "Configuring User Access Controls Overview" on page 17.

You can configure user access control by:

- Deciding how users will be authenticated and authorized to access Junos Space Platform
- Segregating users based on the system functionality they are allowed to access. You can assign a different set of roles to different users. Junos Space Network Management Platform includes more than 25 predefined user roles and allows you to create custom roles that are based on the needs of your organization. When a user logs in to Junos Space, the workspaces that the user can access and the tasks that they can perform are determined by the roles that have been assigned to that particular user account.
- Segregating users based on the domains that they are allowed to access. You can use the Domains feature in Junos Space to assign users and devices to the global domain and create subdomains, and then assign users to one or more of these domains. A domain is a logical grouping of objects, which can include devices, templates, users, and so on. When a user logs in to Junos Space, the set of objects that they are allowed to see is based on the domains to which that user account has been assigned.

  You can use multiple domains to separate large, geographically distant systems into smaller, more manageable sections and control administrative access to individual systems. You can assign domain

administrators or users to manage devices and objects that are assigned to their domains. You can design the domain hierarchy in such a way that a user assigned to one domain need not necessarily have access to objects in another domain. You can even restrict users assigned to a domain from viewing objects that are in the parent domain (in Junos Space Release 13.3, from viewing the objects in the global domain).

For example, a small organization might have only one domain (the global domain) for their entire network, whereas a large, international organization might have several subdomains within the global domain to represent each of its regional office networks across the world.

The following sections describe how to configure a user access control mechanism:

Authentication and Authorization Mode

The first decision to be made is regarding the mode of authentication and authorization that you want. The default mode in Junos Space is local authentication and authorization, which means that you must create user accounts in the Junos Space database with a valid password and assign a set of roles assigned to those accounts. User sessions are authenticated based on this password, and the set of roles assigned to the user account determine the set of tasks the user can perform.

If your organization relies on a set of centralized authentication, authorization, and accounting (AAA) servers, you can configure Junos Space to work with these servers by navigating to the Authentication Servers page in the Administration workspace (**Network Management Platform > Administration**).

NOTE:

- You must have Super Administrator or System Administrator privileges to configure Junos Space to work with these servers.
- You need to know the IP addresses, port numbers, and shared secrets of the remote AAA servers for configuring Junos Space to access them. We recommend that you use the Connection button to test the connection between Junos Space and the AAA server as soon as you add the server in Junos Space. This immediately lets you know whether there is any problem with the configured IP address, port, or credentials.
- You can configure an ordered list of AAA servers. Junos Space contacts them in the order you configured; the second server is contacted only if the first one is unreachable, and so on.

- You can configure RADIUS or TACACS+ servers over Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). You are allowed to have a mix of RADIUS and TACACS+ servers in the ordered list of AAA servers that Junos Space maintains.
- There are two modes of remote authentication and authorization: remote-only and remote-local.
  - *remote-only*—Authentication and authorization are performed by a set of remote AAA servers (RADIUS or TACACS+).
  - *remote-local*—In this case, when a user is not configured on the remote authentication servers, when the servers are unreachable, or when the remote servers deny the user access, then the local password is used if such a local user exists in the Junos Space database.

If you are using remote-only mode, you do not have to create any local user accounts in Junos Space. Instead, you must create user accounts in the AAA servers that you use and associate a remote profile name to each user account. A remote profile is a collection of roles that define the set of functions that a user is allowed to perform in Junos Space. You create the remote profiles in Junos Space. For more information about remote profiles, see "Remote Profiles" on page 23. Remote profile names can be configured as a vendor-specific attribute (VSA) in RADIUS and as an attribute-value pair (AVP) in TACACS+. When an AAA server successfully authenticates a user session, the remote profile name is included in the response message that is sent back to Junos Space. Junos Space looks up the remote profile based on this remote profile name and determines the set of functions that the user is allowed to perform.

Even in the case of remote-only mode, you might want to create local user accounts in Junos Space in either of the following cases:

- You want to ensure that a user is allowed to log in to Junos Space even if all the AAA servers are down. In this case, if a local user account exists in the Junos Space database, the user session is authenticated and authorized based on the local data. You might choose to do this for a few important user accounts for whom you want to ensure access even in this scenario.
- You want to use device partitions to partition a device into subgroups and assign these subobjects to different users. You use device partitions to share the physical interfaces, logical interfaces, and physical inventory elements across multiple subdomains. Device partitions are supported only on M Series and MX Series routers. For more information, see the *Creating Device Partitions* topic in the *Junos Space Network Management Platform* Workspaces User Guide.

For more information about user authentication, see the *Junos Space Authentication Modes Overview* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Certificate–Based and Certificate Parameter–Based Authentication

Junos Space Network Management Platform supports certificate–based and certificate parameter–based authentication for a user. Starting from Release 15.2R1, you can also authenticate users in certificate parameter–based authentication mode. With certificate–based and certificate parameter–based authentication, instead of authenticating a user based on the user's credentials, you can authenticate a user based on the user's certificate and certificate parameters. These authentication modes are considered more secure than password-based authentication. With certificate parameter–based authentication, you can define a maximum of four parameters that are authenticated during the log in process. Certificate–based and certificate parameter–based authentication over an SSL connection can be used to authenticate and authorize sessions among various servers and users. These certificates can be stored on a smart card, a USB drive, or a computer's hard drive. The users typically swipe their smart card to log in to the system without entering their username and password.

For more information about certificate–based and certificate parameter–based authentication, see the *Certificate Management Overview* topic in the Junos Space Network Management Platform Workspaces Feature Guide.

User Roles

When configuring Junos Space, you must decide how you want to segregate users based on the system functionality that users are allowed to access. You do this by assigning a different set of roles to different users. A *role* defines a collection of workspaces that a Junos Space user is allowed to access and a set of actions that the user is allowed to perform within each workspace. To evaluate the predefined user roles that the Junos Space Network Management Platform supports, navigate to the **Roles** page (**Network Management Platform > Role Based Access Control > Roles**). In addition, every Junos Space application that is installed on the Junos Space Network Management Platform has its own predefined user roles. The Roles page lists all existing Junos Space application roles, their descriptions, and the tasks that are included in each role.

If the default user roles do not meet your needs, you can configure custom roles by navigating to the **Create Role** page (**Network Management Platform > Role Based Access Control > Roles > Create Role**). To create a role, you select the workspaces that a user with this role is allowed to access, and for each workspace, choose the set of tasks that the user can perform from that workspace.

NOTE: You might need to go through several iterations of creating user roles to arrive at the optimal set of user roles that your organization needs.

After the user roles are defined, they can be assigned to various user accounts (in the case of local user accounts created in Junos Space) or assigned to remote profiles to be used for remote authorization.

For more information about configuring user roles, see the *Role-Based Access Control Overview* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Remote Profiles

Remote profiles are used in the case of remote authorization. A remote profile is a collection of roles defining the set of functions that a user is allowed to perform in Junos Space. There are no remote profiles created by default, and you need to create them by navigating to the **Create Remote Profile** page (**Network Management Platform > Role Based Access Control > Remote Profiles > Create Remote Profile**). When creating a remote profile, you need to select one or more roles that belong to it. Then you can configure the name of the remote profile for one or more user accounts in the remote AAA servers.

When an AAA server successfully authenticates a user session, the AAA server includes the configured remote profile name for that user in the response message that comes back to Junos Space. Junos Space looks up the remote profile based on this name and determines the set of roles for the user. Junos Space then uses this information to control the set of workspaces the user can access and the tasks the user is allowed to perform.

> **NOTE**: If you decide to use local authorization along with remote authentication, you do not need to configure any remote profiles. In this case, you must create local user accounts and assign roles to these user accounts. The configured AAA servers perform authentication, and for each authenticated session, Junos Space performs the authorization based on the roles configured locally for the user account in the database.

For more information about creating remote profiles, see the *Creating a Remote Profile* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Domains

You can add, modify, or delete a domain from the **Domains** page (**Role Based Access Control > Domains**). This page is accessible only when you are logged in to the global domain, which means that you can add, modify, or delete a domain only from the global domain. By default, any domain you create is added under the global domain. When you add a domain, you can choose to allow users in this domain to have read-only access to the parent domain. If you choose to do so, then all users in the subdomain can view objects of the parent domain in read-only mode.

NOTE: Only two levels of hierarchy are supported: the global domain and any other domains that you might add under the global domain.

For more information about managing domains, see the *Domains Overview* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

User Accounts

You need to create user accounts in Junos Space in the following cases:

- To perform local authentication and authorization—You create user accounts in Junos Space. Each user account must contain a valid password and a set of user roles. To create user accounts, navigate to the **Create User** page (**Network Management Platform > Role Based Access Control> User Accounts > Create User**).
- To perform remote authentication and local authorization—You create a user account for each user of the system and ensure that a set of roles is assigned to each user account. It is not mandatory to enter a password for the user accounts because authentication is performed remotely.
- To perform remote authentication and authorization and allow certain users to be able to access Junos Space even if all AAA servers are down or are not reachable from Junos Space—You create local user accounts for these users with a valid password. The system forces you to configure at least one role for these users. However, authorization is performed based on the remote profile name that the AAA server provides.
- To perform remote authentication and authorization but also override remote authentication failures for specified users and allow them to access Junos Space— A typical scenario would be when you need to create a new Junos Space user but do not have immediate access to configure the user on the remote AAA servers. You must create local user accounts for such users with a valid password and a valid set of roles.
- To perform remote authentication and authorization but also segregate devices among users based on domains—Because domains must be assigned to user objects in Junos Space, you must create remote profiles in Junos Space and assign roles and domains to those profiles.

  NOTE: If you decide to use local authorization along with remote authentication, you do not need to configure any remote profiles. In this case, you must create local user accounts and assign roles to these user accounts. The configured AAA servers perform authentication, and

for each authenticated session, Junos Space performs the authorization based on the roles configured locally for the user account in the database.

NOTE: Junos Space enforces certain rules for valid passwords. You configure these rules as part of the Network Management Platform settings from the **Applications** page (**Network Management Platform > Administration > Applications**). Right-click the application and select **Modify Application Settings**. Then select **Password** on the left side of the window. On the subsequent page, you can view and modify the current settings.

For more information about creating user accounts, see the *Creating Users in Junos Space Network Management Platform* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Device Partitions

You can partition a device from the **Devices** page (**Network Management Platform > Devices > Device Management**). You can partition a device into subgroups and then assign these subobjects to different users by assigning the partitions to different domains. Only one partition of a device can be assigned to a domain.

NOTE: Device partitions are supported only on M Series and MX Series routers.

For more information about device partitions, see the *Creating Device Partitions* topic (in the *Junos Space Network Management Platform* Workspaces User Guide).

Release History Table

Release	Description
15.2R1	Starting from Release 15.2R1, you can also authenticate users in certificate parameter–based authentication mode.

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 10

Backing Up the Junos Space Platform Database | 16

CHAPTER 3

Junos Space Network Management

Device Management in Junos Space Platform

IN THIS SECTION

When using Junos Space to manage your network, you must first discover the devices in your network through a device discovery profile, add these devices to the Junos Space Platform database, and allow the devices to be managed by Junos Space Platform. When devices are successfully discovered and managed by Junos Space Platform, the following actions occur:

- A dedicated Device Management Interface (DMI) session is established between Junos Space and each device. This DMI session typically rides on top of an SSHv2 connection with the device. For devices running the export version of Junos OS (ww Junos OS devices), DMI uses a Telnet connection through the wwadapter. The DMI session is maintained till the device is deleted from Junos Space, which means that the session is reestablished in case of transient network problems, device reboots, Junos Space restarts, and so forth.
- When the network itself is the system of record (NSOR), Junos Space imports the complete configuration and inventory of the device into its own database. To keep device information current, Junos Space listens to system log events raised by the device that indicate device configuration or inventory changes, and Junos Space automatically resynchronizes its database with the latest information from the device. When the Junos Space Network Management Platform is the system of record (SSOR), Junos Space reflects the changes on the device, but a Junos Space user with appropriate user privileges must resolve out-of-band changes.
- By default, Junos Space adds itself as an SNMP trap destination by automatically inserting the appropriate SNMP configuration on the device during device discovery; however, you can disable this behavior from the **Network Management Platform > Administration > Applications Network Management Platform > Modify Application Settings** page.
- Junos Space uses SNMP polling to collect key performance indicators (KPIs) from the devices. To enable SNMP polling on managed devices requires that the Network Monitoring feature be turned on.

NOTE: By default, Junos Space Network Monitoring is turned on for all devices.

NOTE: Starting from Release 16.1R1, you can use a NAT server to discover and manage devices that are outside your Junos Space network and which cannot reach Junos Space Platform. When you add a NAT configuration on the **Administration > Fabric > NAT Configuration** page and forwarding rules on the NAT server, the IP addresses translated through the NAT server are added to the outbound ssh stanza of the external devices.

The following sections list the device management capabilities of Junos Space Platform:

Discovering Devices

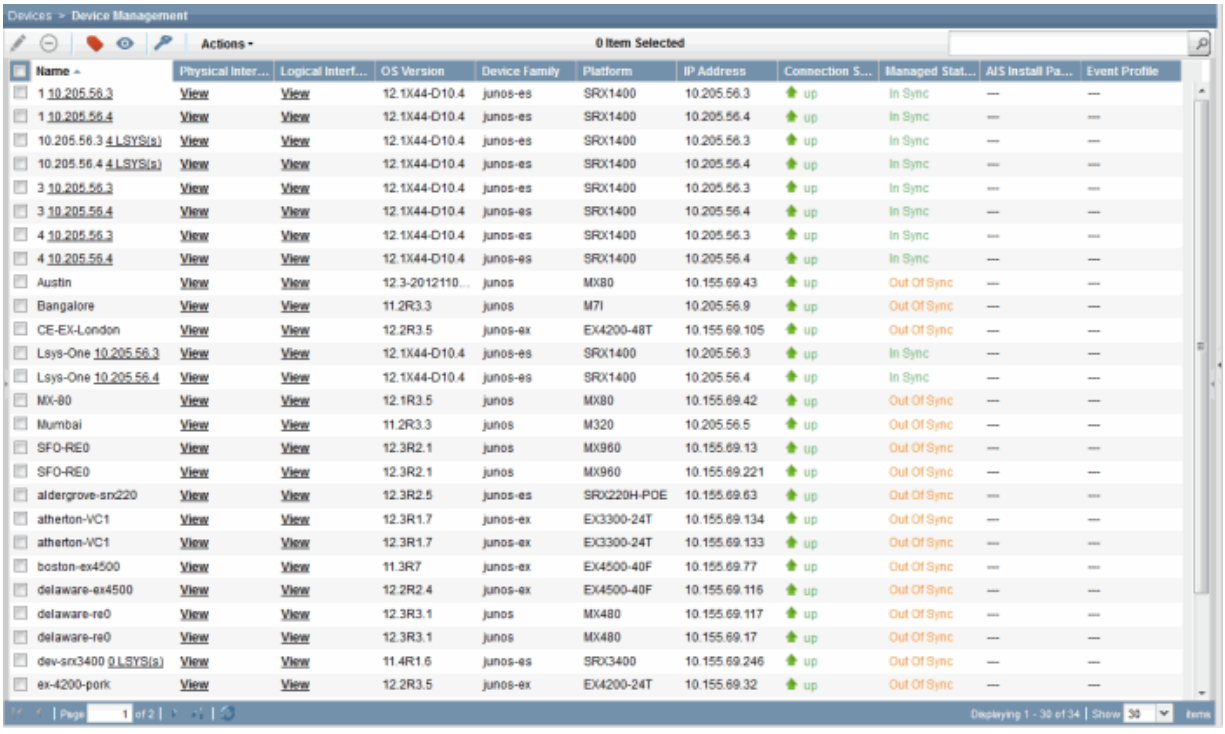
Before you can discover devices into Junos Space, ensure the following:

- You know the key details about the devices to discover. You provide this information as input to discover devices:
  - Device details–IP address or hostname of the device or subnet to scan
  - Credentials–User ID and password of a user account that has appropriate user privileges on the device
  - SNMP Credentials–Community string with read-only access if you are using SNMPv2c or valid SNMPv3 credentials. SNMP credentials are not required if you do not plan to use Junos Space to monitor faults and performance of managed devices.
- The IP address of the device can be reached from your Junos Space server.
- SSHv2 is enabled on the device (`set system services ssh protocol protocol-version v2`) and any firewalls along the way allow Junos Space to connect to the SSH port (default TCP/22) on the device. To discover devices running the export version of Junos OS, the wwadapter must be installed on Junos Space and Telnet must be enabled on the device and reachable from Junos Space.
- SNMP port (UDP/161) on the device is accessible from Junos Space, which allows Junos Space to perform SNMP polling on the device to collect KPI data for performance monitoring.
- SNMP trap port (UDP/162) on Junos Space is accessible from the device, which allows the device to send SNMP traps to Junos Space for fault management.

Starting from Release 16.1R1, you can create a device discovery profile (in the Devices workspace) to set preferences for discovering devices. After verifying the prerequisites, you create a device discovery profile from the **Network Management Platform > Devices > Device Discovery Profiles** page. The device discovery profile contains the preferences to discover devices, such as, device targets, probes, authentication details, SSH credentials, and a schedule at which the profile should be run to discover devices. You can also manually run the device discovery profile from the **Network Management Platform > Devices > Device Discovery Profiles** page. The time required to complete the discovery process depends on multiple factors such as the number of devices you are discovering, the size of configuration and inventory data on the devices, the network bandwidth available between Junos Space and the devices, and so forth.

After your devices are successfully discovered in Junos Space, you can view the devices from the **Network Management Platform > Devices > Device Management** page. The Connection Status for the discovered devices should display “Up” and the managed status should be “In Sync” as shown in Figure 4 on page 29, which indicates that the DMI session between Junos Space and the device is up and that the configuration and inventory data in Junos Space is in sync with the data on the device.

Figure 4: Device Management Page



For complete information about discovering and managing devices, see the Devices workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Authenticating Devices

Starting from Release 16.1R1, new enhancements to device authentication are introduced. Junos Space Network Management Platform can authenticate a device by using credentials (username and password), 2048 bit or 4096 bit keys (which uses public-key cryptographic principles such as RSA, DSS, ECDSA), or the device's SSH fingerprint. You can choose an authentication mode on the basis of the level of security needed for the managed device. The authentication mode is displayed in the Authentication Status column on the Device Management page. You can also change the authentication mode. You need to ensure the following to use these modes of authentication:

- Credentials-Based–Device login credentials with administrative privileges are configured on the device before the device connects to Junos Space Platform.
- Key-Based (keys generated by Junos Space Platform)–By default, a Junos Space installation includes an initial public and private key pair. You can generate a new key pair from the Administration workspace and upload the Junos Space's public key to the devices that are to be discovered from the Devices workspace. Junos Space logs in to these devices through SSH and configures the public key on all the devices. You need not specify a password during device discovery; you need to specify only the username.
- Custom key-based–A private key and an optional passphrase. You can upload the private key to Junos Space Platform and use the passphrase to authenticate the private key. You don't need to upload the private key to devices.

For complete information about device authentication, see the Devices workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Viewing the Device Inventory

Junos Space Platform maintains up-to-date inventory details of all managed devices in the database. This includes the complete hardware, software, and license inventory of each device as well as details of all physical and logical interfaces on these devices. You can resynchronize a managed device with the Junos Space Platform database to fetch the current configuration and inventory details.

You can view and export hardware, software, and license inventory details, and the physical and logical interfaces of a device from the Junos Space user interface. You can acknowledge the inventory changes on a device from the Junos Space user interface. For complete information about these tasks, see the Devices workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Upgrading Device Images

Junos Space Platform can be a central repository for all device OS images and provide workflows to download and install these images on managed devices. You can upload, stage, and verify the checksum of device images, and deploy device images and Junos Continuity software packages to a device or multiple devices of the same device family simultaneously from the Images and Scripts workspace. For complete information about upgrading device images, see the Images and Scripts workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Release History Table

Release	Description
16.1R1	Starting from Release 16.1R1, you can use a NAT server to discover and manage devices that are outside your Junos Space network and which cannot reach Junos Space Platform.
16.1R1	Starting from Release 16.1R1, you can create a device discovery profile (in the Devices workspace) to set preferences for discovering devices.
16.1R1	Starting from Release 16.1R1, new enhancements to device authentication are introduced.

RELATED DOCUMENTATION

DMI Schema Overview | 15

Device Configuration Management in Junos Space Platform

IN THIS SECTION

Junos Space Platform maintains an up-to-date database copy of the complete configuration of each managed device. You can view and modify the device configurations from the Junos Space user interface. Because a Junos device configuration is described in terms of an XML schema and Junos Space Platform has access to this schema, Junos Space user interface uses this schema to graphically render the device configuration. With an up-to-date schema, you can view and configure all configuration options as you would modify the configuration from the device CLI.

By default, Junos Space Platform operates in the mode where it considers the network as the system of record (NSOR). In this mode, Junos Space Platform listens to all configuration changes on managed devices and automatically resynchronizes its database copy with the modified device configuration to reflect the changes. You can change this to a mode where Junos Space considers itself as the system of record (SSOR). In this mode, Junos Space Platform does not automatically synchronize its copy of the device configuration with the modified device configuration when it receives information about out-of-band configuration changes made on a managed device. Instead, the device is marked as *Device Changed* and you can view the changes and decide whether to accept the changes. If you accept the changes, the changes are written into the Junos Space Platform database copy of the device configuration. If you reject the changes, Junos Space Platform removes the configuration from the device. For complete information about NSOR and SSOR modes, see the Devices workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

The following sections list the device configuration management capabilities of Junos Space Platform:

Modifying the Device Configuration by Using the Schema-Based Configuration Editor

You modify the configuration on a single device by using the Schema-based Configuration Editor. To modify a device configuration on a device, right-click the device listed on the Device Management page (in the Devices workspace) and select **Modify Configuration**. You can view the following details:

- Current configuration on the device
- Tree view of the device's configuration hierarchy. Click and expand this tree to locate the configuration stanzas of interest. For more information about the configuration options on a device, refer to Junos OS technical documentation.
- Options to filter the configuration and search for specific configuration options in the tree
- Details of a configuration node when you click the node in the tree
- Options to create, edit, delete, and order entries on the list when you navigate within a configuration node

- Options to view information about individual parameters (blue information icons), add comments about individual parameters (yellow comment icons), and activate or deactivate a configuration option
- Options to preview, validate, and deploy the configuration to the device

For complete information about modifying and deploying the configuration by using the Schema-based Configuration Editor, see the Devices workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Modifying the Device Configuration by Using Device Templates

You may need to create a common configuration change and push it to multiple devices. You can use the Device Templates feature in Junos Space Platform to create and deploy changes from the Junos Space user interface. You first create a template definition to restrict the scope of a device template to a specific device family and Junos OS version. You then create a device template by using the template definition. You can also create and deploy a configuration by using Quick templates (without using a template definition). You can validate the templates, view the configuration in multiple formats, and deploy (or schedule the deployment of) the configuration to multiple devices. For complete information about creating and deploying a configuration to devices by using device templates, see the Device Templates workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Viewing Configuration Changes

Junos Space Platform tracks all the configuration changes (from the Schema-Based Configuration Editor, Device Templates feature, Junos Space applications, or the device CLI) made on managed devices. You can view the list of configuration changes on the device in multiple formats from the Junos Space user interface. To view the list of configuration changes, right-click the device and select **View Configuration Change Log**. Each configuration change log entry includes details such as the timestamp of change, user who made the change, the configuration change in XML format, whether the change was made from Junos Space or out-of-band, and also the name of the application or feature that was used to change the configuration. If you have set up Junos Space Platform as the system of record, out-of-band configuration changes on a device modify the managed status of the device to *Device Changed*. You can view and resolve such out-of-band changes by selecting the device and selecting Resolve Out-of-band Changes. You can view a list of all out-of-band changes made on the device. You can accept or reject the changes.

For complete information about viewing configuration changes, see the Device Templates workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

Backing Up and Restoring Device Configuration Files

Junos Space Platform allows you to maintain multiple versions of device configuration files (running, candidate, and backup configuration of managed devices) in the Junos Space Platform database. You can recover device configuration files in case of a system failure and maintain consistent configuration across multiple devices. You can select and back up the configuration from multiple devices from the Configuration Files workspace. A separate configuration file is created in the database for each managed device. For complete information about backing up and restoring device configuration files, see the Configuration Files workspace documentation in the *Junos Space Network Management Platform* Workspaces User Guide.

RELATED DOCUMENTATION

DMI Schema Overview | **15**