



Junos[®] Space

Edge Services Director Quick Start Guide

Release

1.0



Modified: 2018-07-23

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

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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

Junos® Space Edge Services Director Quick Start Guide

1.0

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

Edge Services Director Installation Overview	1
Configuring Basic Junos Space Settings	2
Upgrading Junos Space	5
Junos Space Network Management Platform Requirements for Junos Space Edge Services Director	6
Junos Space SDG DMI Schema Requirements for Junos Space Edge Services Director	8
Installing Edge Services Director	10
Upgrading Edge Services Director	13
Uploading DMI Schemas	14
Preparing Devices for Management by Edge Services Director	16
Discovering Devices	16
Preparing MX Series Devices for Discovery	17
Specifying a Discovery Profile and the Target Devices	18
Specifying SNMP Probes	21
Specifying Credentials	24
Getting Started with Edge Services Director	25
Next Steps	28
Edge Services Director REST API Overview	29
Format and Conventions of RESTful Web Services	32

Edge Services Director Installation Overview

Junos Space Edge Services Director enables unified management of services on Juniper Networks MX240, MX480, and MX960 3D Universal Edge routers. Service providers are increasingly using IP Layer 3 through Layer 7 services to differentiate themselves from third-party, external providers and provide a better user experience. These IP services manage traffic flow per application type, enhance security, improve video quality and offer other enhanced IP applications. The service delivery gateway (SDG) (running on the MX Series router) consolidates a variety of network services onto a single platform to reduce cost and increase network resiliency.

Services interfaces, such as adaptive services interfaces and multiservices interfaces, provide specific capabilities for manipulating traffic before it is delivered to its destination. Edge Services Director is a cohesive and robust GUI application that you can use on a server that is running the Junos Space Network Management Platform software.

You can use the Edge Services Director application to add SDGs, which are MX Series routers, discover SDGs into the Edge Services Director database, and manage the SDG settings. Currently, for the Edge Services Director Release 1.0, which is the first implementation of this application, stateful firewall, carrier-grade Network Address Translation (CGNAT), and load balancing services are supported. You can configure and deploy these services to a large number of SDGs for easy and effective administration. Using the Edge Services Director application, you can also configure policies and filters for these services to classify and forward traffic traversing the SDGs.

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

You can install Edge Services 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 Edge Services Director as an application. 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 Edge Services Director on a Junos Space JA2500 Appliance:

- [Configuring Basic Junos Space Settings](#)
- [Upgrading Junos Space on page 5](#)
- [Junos Space SDG DMI Schema Requirements for Junos Space Edge Services Director on page 8](#)
- [Junos Space Network Management Platform Requirements for Junos Space Edge Services Director on page 6](#)
- [Installing Edge Services Director](#)
- [Upgrading Edge Services Director on page 13](#)
- [Uploading DMI Schemas](#)
- [Preparing Devices for Management by Edge Services Director](#)
- [Discovering Devices](#)
- [Getting Started with Edge Services Director](#)
- [Next Steps](#)

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.



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.



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-junospace-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

Edge Services Director Release 1.0 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 Edge Services 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 Edge Services 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 15.1 supports upgrading from Release 14.1 or 13.3. 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?](#).

Junos Space Network Management Platform Requirements for Junos Space Edge Services Director

The Edge Services Director Release 1.1 GUI is supported on Junos Space Network Management Platform Release 15.2R2.

Edge Services Director is supported on a JA2500 Junos Space Appliance or a Junos Space Virtual Appliance that meets the hardware requirements specified in the Junos Space documentation. The number of devices you plan to manage by using Edge Services Director determines which Junos Space Appliance to use. Contact Juniper Networks Technical Assistance Center to know more about the Junos Space Appliance model that is suitable for your network. Edge Services Director is not supported on a Junos Space instance running on a Juniper Networks NSM3000 appliance.

You can install Edge Services 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 Connectivity Services Director and the API as an application. The Junos Space Appliance has been tested with up to six appliances connected in a cluster (fabric) for its ability to manage up to 15,000 devices. The Junos Space architecture also achieves five-nines reliability.

The JA2500 appliance has a 2-U, rack-mountable chassis with dimensions 17.81 in. x 17.31 in. x 3.50 in. (45.20 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 the installation of an operating system and applications to become fully functional.

The Junos Space Virtual Appliance can be deployed on a VMware ESX server. The Junos Space Virtual Appliance requires a VMware ESX server 4.0 or later or VMware ESXi server 4.0, 5.0, 5.1, or 5.5 that can support a virtual machine with the following configuration:

- 64-bit quad processor with at least 2.66-GHz speed
- 32-GB RAM
- One RJ-45 10/100/1000 Network Interface Connector
- 100-GB hard disk

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](#).

Related •
Documentation

Junos Space SDG DMI Schema Requirements for Junos Space Edge Services Director

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 situations, you must obtain and upload the requisite schema and set it as the default DMI schema for each device family. For the service delivery gateways (SDGs), which are running on MX Series routers, you can set a default SDG DMI schema for each device family to enable Junos Space to apply an appropriate schema to a device family.



NOTE: See [Setting a Default DMI Schema](#) for detailed steps to set a default schema.

Table 1 on page 8 lists the latest SDG DMI schema that you must obtain and upload in Junos Space before you start working on Edge Services Director Release 1.1.

Table 1: SDG DMI Schemas

Device	Name of the SDG DMI Schema	Device Family
MX240 MX480 MX960	JUNOS 14.1X55-D25	junos-mx

After you obtain the DMI schema, to install the schema update on Junos Space Platform if you already have the compressed TAR file (extension **.tgz**) available:

1. On the Junos Space Network Management Platform user interface, select **Administration > DMI Schemas**

The DMI Schemas page appears.

2. Click the **Update Schema** icon on the toolbar.

The **Update Schema** page appears.



NOTE: On the Update Schema page, Junos Space Platform displays the schemas that you already have installed and, based on the discovered devices, suggests new schemas. However, you can pick other available schemas and download them.

3. Select the **Archive (tgz)** option button.

4. Click **Browse**.

The **File Upload** dialog box appears.

5. Select the compressed TAR file (extension **.tgz**) and click **Open**.

The **Update Schema** page reappears, displaying the compressed TAR file (extension **.tgz**) in the **Archived Schemas File** field.

6. Click **Upload**.



NOTE: Do not move away from the **Update Schema** page while the compressed TAR file (extension **.tgz**) is being uploaded to Junos Space Platform. The time taken for the upload process depends on the number of schemas in the file. A progress bar indicates the percentage of the upload that has completed.

To update the DMI schema directly from the Juniper Networks DMI schema repository:

1. Select the **SVN Repository** option button.

If the access to the Juniper Networks Subversion repository is already configured, the URL of the repository is displayed in the **URL** field. If the access is not configured, a note indicating that the access must be configured is displayed.

To configure access to the Juniper Networks Subversion repository:

- a. Click **Configure**.

The **SVN Access Configuration** dialog box appears.

- b. In the **Svn URL** field, enter the URL of the Juniper Networks Subversion repository (<https://xml.juniper.net/dmi/repository/trunk/>).
- c. In the **User Name** field, enter the user name to access the Juniper Networks Subversion repository.
- d. In the **Password** field, enter the password to access the Juniper Networks Subversion repository.
- e. In the **Confirm** field, reenter the password to access the Juniper Networks Subversion repository.
- f. (Optional) The **Proxy Server** field displays whether a proxy server is configured or not. If your organization requires that you use a proxy server to connect to the Internet, you must configure and enable the proxy server (under **Administration** > **Proxy Server**) before connecting to the Juniper Networks Subversion repository.
(Optional) Click **Test Connection**.

A message dialog box appears (after a few seconds or a few minutes depending on the connection) to indicate whether the connection is established successfully or not. Click **OK** to close the dialog box and return to the **Svn Access Configuration** dialog box.

- g. Click **Save** to save the settings that you configured.

You are taken to the Update Schema page and the URL that you configured is displayed in the **URL** field.

2. (Optional) From the **Device Family** drop-down list, select the device families that you want to download from the repository.



NOTE: If you do not specify a device family, then available schemas from all families are listed.

3. Click **Connect**.

Junos Space Platform displays a message asking you to wait while the list of schemas is retrieved. (This process might take anywhere from a few seconds to a few minutes depending on the connection.)

For detailed steps for acquiring and uploading the schema files, see [Managing DMI Schemas Overview](#).

Installing Edge Services Director

Before you begin:

- Edge Services Director is supported on a JA2500 Junos Space Appliance or a Junos Space Virtual Appliance that meets the hardware requirements specified in the Junos Space documentation. The number of devices you plan to manage by using Edge Services Director determines which Junos Space Appliance to use.
- If Edge Services Director Release 1.0 is installed on the Junos Space Appliance, then you must uninstall it and restart JBoss before installing Edge Services Director Release 1.1.
- You cannot install Network Director or Connectivity Services Director on the same system as Edge Services Director. Uninstall Network Director or Connectivity Services Director before you install Edge Services Director on your system.
- 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 Edge Services Director Download](#) page.

- Download Edge Services Director Release 1.0 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 Edge Services Director version to either the hard disk or to an SCP server. The Edge Services Director software images are located at the [Junos Space and Junos Space Edge Services Director Download](#) page.

1. Install or upgrade to a supported release of Network Management Platform. See [“Junos Space Network Management Platform Requirements for Junos Space Edge Services Director” on page 6](#) for requirements information.

2. Install Edge Services Director Release 1.1.

After the installation is complete, the system includes Edge Services Director in the list of installed applications.

To install Edge Services 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 Edge Services Director by using HTTP:

- a. Click **Upload via HTTP** to open the dialog box.
- b. Navigate to the local location where the Edge Services 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 Edge Services 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 Edge Services Director application file.

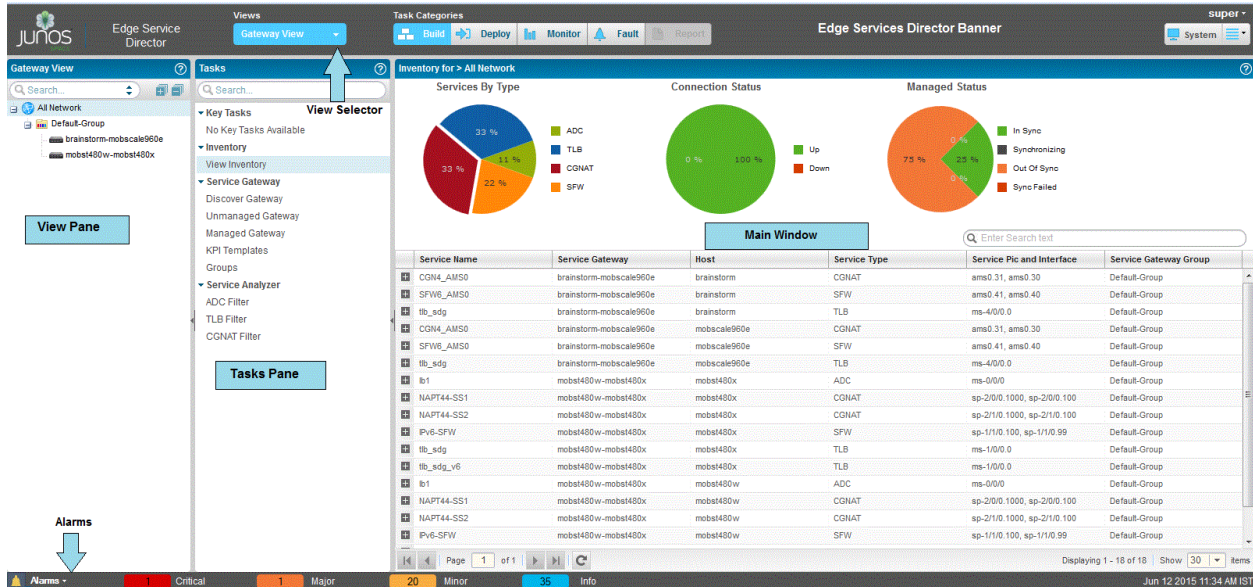
- c. Click **Upload** to load the image file into Junos Space.
3. Click **OK** to skip viewing the job results.
4. Select **Edge Services Director** and click **Install**.
5. Click **OK** in the Application Configuration window dialog box.

You can check the Job Status page to view the progress of the installation job. Once the installation completes, Edge Services 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.
7. To work with Edge Services Director, select **Edge Services Director** from the Applications list in the upper left corner above the Tasks tree.

Edge Services Director starts in your browser window and opens the default view as shown in [Figure 1 on page 12](#).

Figure 1: Edge Services Director Interface



8. Bookmark this page in your browser for future use.

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

9. Do the following depending on your networking requirements:
 - a. Perform the initial configuration of Edge Services Director. See *Preparing Devices for Management by Connectivity Services Director*.

Upgrading Edge Services Director

You can upgrade Edge Services Director from Release 1.0R1 to Edge Services Director Release 1.1.

Before you start the upgrade, ensure that you have:

- Taken a backup of your database by using the Junos Space backup feature. For more details, see [Backing Up and Restoring the Database Overview](#).
- Junos Space Release 15.2R2 running on your appliance. If your appliance is running an unsupported release of Junos Space, you must upgrade Junos Space before installing Edge Services Director.
- Downloaded the Edge Services Director Release 1.1 software image to the hard disk or to an SCP server. The Edge Services Director software images are located at <http://www.juniper.net/support/downloads/spaceesd.html>.
- Ensure that Junos Space Network Management Platform Release 15.2R2 is running.

1. Install Edge Services Director Release 1.1.
2. 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
```



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.

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.

[Table 2 on page 15](#) lists the latest SDG DMI schema that you must obtain and upload in Junos Space before you start working on Edge Services Director Release 1.0.

Table 2: SDG DMI Schemas

Device	Name of the SDG DMI Schema	Device Family
MX240 MX480 MX960	JUNOS 14.1X55-D25	junos-mx

If you cannot find an appropriate schema for your device model, contact Juniper Support.

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 Edge Services Director

To discover and manage devices, Edge Services 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. Issue the **set system services ssh protocol-version v2** command to enable SSH v2 on M, MX, and PTX Series routers.
- Has a user ID with the superuser class configured. Junos Space, and Edge Services 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; Edge Services Director configures traps as a deployment task.

In addition, the following protocol ports must be open for Edge Services 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 162 for service-level SNMP traps. Edge Services Director uses OpenNMS for SNMP trap collection and correlation.
- Port 21 (TCP) and port 69 (UDP) for uploading the software image and configuration file to the FTP server.

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 162 is open on a device issue this command:

```
root@space# nmap <IP address of device> -p 162
```

Discovering Devices

You can discover and synchronize physical devices such as MX Series routers that function as service delivery gateways in your network that are managed by Edge Services Director.



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

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

While in Build mode, from the Tasks pane, select **Service Gateways**. The Service Gateways page is displayed. Click **Discover Devices** to create a discovery profile or a job, and to view the previously created discovery profiles

This topic describes:

- [Preparing MX Series Devices for Discovery on page 17](#)
- [Specifying a Discovery Profile and the Target Devices on page 18](#)
- [Specifying SNMP Probes on page 21](#)
- [Specifying Credentials on page 24](#)

Preparing MX Series Devices for Discovery

Juniper Networks MX Series 3D Universal Edge Routers—MX240, MX480, and MX960—include all standard Ethernet capabilities as well as enhanced mechanisms for service providers to provision and support large numbers of Ethernet services in addition to all Layer 3 services. You can discover these routers and manage them as switching devices from Edge Services Director. However, before discovering these MX devices from Edge Services Director, you must ensure that the Junos OS running on the device is at the required level and that the network service mode is set to LAN.

To prepare an MX Series device for discovery:

1. Log in to the MX Series device by using the CLI.
2. Ensure that the device is running a version of Junos OS that is compatible with Edge Services Director. Use the operational mode command **show version** to determine the Junos OS software release.
3. Commit your changes.

The MX Series device is now discoverable from Edge Services Director.

Specifying a Discovery Profile and the Target Devices

You can add devices to Edge Services Director for device discovery by using the **Add** icon on the Service Gateways page. A discovery profile is created, which is a discovery job that contains the list of devices and its properties to be retrieved and added to the Edge Services Director database.



NOTE: If you want to discover and manage MX Series devices—MX240, MX480, and MX960—from Edge Services Director, you must first make these devices discoverable. For more details see [“Preparing MX Series Devices for Discovery” on page 17](#).

To specify a discovery profile and the target devices that you want Edge Services Director to discover:

1. From the View selector, select **Gateway View**. The workspaces that are applicable to this view are displayed.
2. From the Junos Space user interface, click the **Build** icon on the Edge Services Director banner.
The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View selector, select **Gateway View** or **Device View**. The workspaces that are available in this view are displayed. The Gateway view displays the service delivery gateway (SDG) groups and the SDGs that are part of the high availability pair in an SDG group. The Device view displays the SDGs based on the device type, and within the device type, the devices are organized by the device model. For example, all models of MX960 routers are grouped together under one node in the tree.
4. From the Junos Space user interface, click the **Build** icon on the Edge Services Director banner.
The functionalities that you can configure in this mode are displayed in the task pane.
5. From the View pane, select the All Network item in Gateway view. If you are in Device view, click the plus sign (+) beside the My Network item in the View pane to expand the tree and select the device node you want.

6. From the task pane in Gateway view, select **Services Gateways**.

The Service Gateways page is displayed.



NOTE: Alternatively, you can select **Device View** from the View selector, click the **Build** icon on the banner, and select **Discover Devices** from the task pane to open the Discovery Profiles window to discover and manage devices.

Discovery Profiles							
<div> + Add ✎ Edit ✖ Delete 📄 View 🔄 Discover Now 📅 Schedule </div> <div> <input type="text" value="Enter Search text"/> </div>							
DiscoveryProfile	Description	Created By	Created Time	Modified Time	Last Execution Status	In Progress	Scheduled
<input type="checkbox"/> MX_480_SDG	MX_480_SDG	super	Oct 01, 2015 2:15:22 ...	Nov 03, 2015 9:47:53 ...	Failed on Fri Oct 30 20...	No Instance Running	1 Instance(s) Scheduled
<input type="checkbox"/> MX_960_SDG	MX_960_SDG	super	Oct 01, 2015 2:17:21 ...	Oct 30, 2015 3:47:16 P...	Cancelled on Fri Oct 3...	No Instance Running	No Instance Scheduled
<input type="checkbox"/> MC_Kodiak	MC_Kodiak	super	Oct 01, 2015 2:26:42 ...	Oct 01, 2015 2:30:59 ...	Failed on Thu Oct 01 2...	No Instance Running	No Instance Scheduled
<input type="checkbox"/> deployment-plan-prof	deployment-plan-prof		Oct 27, 2015 5:12:38 P...	Oct 28, 2015 3:32:21 P...	Completed on Wed Oct...	No Instance Running	No Instance Scheduled
<input type="checkbox"/> hamsa		super	Oct 29, 2015 11:53:54 ...	Oct 29, 2015 11:54:27 ...	Completed on Thu Oct...	No Instance Running	No Instance Scheduled
<input type="checkbox"/> TestDevice	TestDeviceDescription	super	Oct 30, 2015 11:55:20 ...	Nov 03, 2015 9:48:38 ...	Failed on Fri Oct 30 20...	No Instance Running	2 Instance(s) Scheduled
<input type="checkbox"/> Automation_Gateway_...	Discover Device Auto...	super	Nov 02, 2015 1:00:24 ...	Nov 02, 2015 1:01:25 ...	Completed on Mon Nov...	No Instance Running	No Instance Scheduled

Page 1 of 1
 Displaying 1 - 7 of 7
Show 24 Items

- From the task pane, select the **Discover Gateway** option. You need not click this button if you are launching the Service Gateways page by navigating from another page or another mode, such as Deploy or Monitor. It is displayed by default. You must click this button only if you are viewing unmanaged or managed SDGs or devices.

- Click the **Add** icon. The Discovery Profile window appears.

Discovery Profile

Name: MX_960_SDG

Description: MX_960_SDG

IP Details

10.213.0.195
 10.213.2.163

User Details

user

SNMP Details

SNMPV2

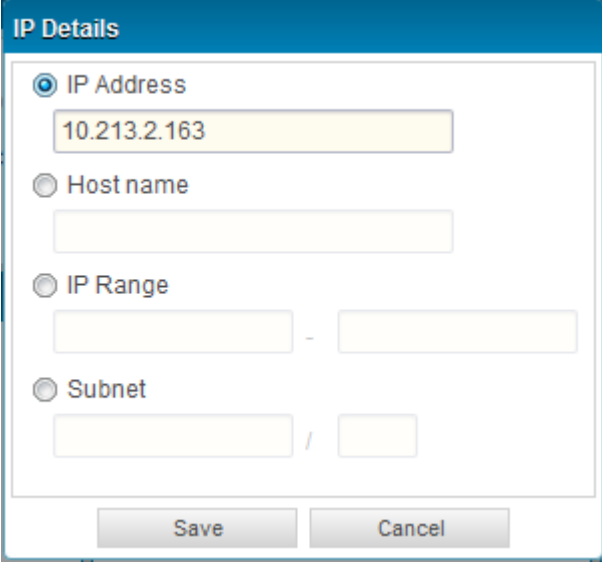
Save

Cancel

- In the **Name** field, enter a name for the device discovery job. No name is shown by default. A job or profile name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quote ('), forward slash (/), and ampersand (&).

10. (Optional) In the **Description** field, type a user-defined description. (a minimum of 2 characters and a maximum limit of 255 characters). The description cannot exceed 256 characters and cannot contain hyphens. The operators who use the profile rely on the description for information on the discovery job.
11. To add individual devices by specifying the IP address credentials, click **Add** in the IP Details table.

The IP Details dialog box appears.

The image shows a dialog box titled "IP Details" with a blue header bar. Inside the dialog, there are four radio button options: "IP Address" (selected), "Host name", "IP Range", and "Subnet". Each option has a corresponding text input field. The "IP Address" field contains the text "10.213.2.163". The "IP Range" field is split into two boxes separated by a hyphen. The "Subnet" field is split into two boxes separated by a slash. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

12. Choose one of the following options to specify the target devices:
 - Select the **IP Address** option and enter the IP address of the device.
 - Select the **IP-Range** option and enter a range of IP addresses for the devices. The maximum number of IP addresses for an IP range target is 1024.
 - Select the **IP-Subnet** option and enter an IP subnet for the devices.
 - Select the **HostName** option and enter the hostname of the device.
 - Click **Save** to save the target devices that you specified. When you have added all target devices that you want Edge Services Director to discover, click **Save** in the Discovery Profile window.

The IP Details section displays the addresses of the configured target devices.

13.
 - To edit a target device, select the box that displays with an icon for each added device in the IP Details section and click **Edit**. Make the required changes and click **Add** to display the IP addresses in the Device Targets table
 - To delete a target device, select the box that displays with an icon for each added device in the IP Details section and click **Delete**.

- To view and download a sample CSV file, click **CSV Sample**. The Opening Device_Discovery_CSV.csv file dialog box is displayed. You can open the sample CSV file or save the sample CSV file.
14. (Optional) You can proceed to specify the SNMP probes and credentials for the added devices.

Specifying SNMP Probes

You can specify an SNMP probe to connect to and discover the devices in a network.

To add a probe:

1. From the View selector, select **Gateway View**. The workspaces that are applicable to this view are displayed.
2. From the Junos Space user interface, click the **Build** icon on the Edge Services Director banner.
The functionalities that you can configure in this mode are displayed in the task pane.
3. From the task pane, select **Services Gateways**. The Service Gateways page is displayed.
4. Select the **Discover Gateway** option.
5. Click the **Add** icon. The Discovery Profile window appears.
6. Click the **Add** icon in the SNMP Details table. The SNMP Details dialog box is displayed.



The image shows the 'SNMP Details' dialog box. It has a blue header with the title 'SNMP Details'. Below the header, there are two radio buttons: 'SNMP V1/V2' (which is selected) and 'SNMP V3'. Under 'SNMP V1/V2', there is a 'Community' label and a text input field containing the word 'public'. Under 'SNMP V3', there are several fields: 'User Name' (empty), 'Privacy' (a dropdown menu showing 'None'), 'Privacy Password' (empty), 'Auth Type' (a dropdown menu showing 'None'), and 'Auth Password' (empty). At the bottom of the dialog box, there are two buttons: 'Save' and 'Cancel'.

7. Select one of the following options and enter the appropriate value in the field provided.
 - Select **SNMP V1/V2C** and specify the community string in the **Community** field.

The SNMP v1/v2c community string *public* is available by default. The SNMP v1/v2c community string is based on the community string configured on the devices in your network.

- Select **SNMP V3** and enter the information in the fields provided.
 - a. Enter the SNMP V3 username in the **Username** field.
 - b. Select the privacy protocol (the encryption standard for the SNMP user) from the **Privacy type** list.
The available options are **AES128**, **DES**, and **None**.
 - c. Enter the password used to generate the key used for encryption in the **Privacy password** field.
The password must be at least eight characters long. You can include all character classes in a password (alphabetic, numeric, and special characters) except control characters.
 - d. Select the authentication type for the SNMP user from the **Privacy type** drop-down list.
The available options are **MD5**, **SHA1**, and **none**.
 - e. Enter the password used to generate the key used for authentication in the **Authentication password** field.
The password must be at least eight characters long. You can include all character classes in a password (alphabetic, numeric, and special characters) except control characters.

8. Click **Save** to close the **SNMP Details** dialog box and add the SNMP probe to the **SNMP Settings** list.

The **SNMP Details** section of the Discovery Profile page displays the configured SNMP settings.

You can also click **Cancel** to close the **SNMP Details** dialog box without adding any SNMP probes.

To edit an SNMP probe:

1. Select the SNMP probe that you want to edit and click the **Modify** icon [slanted pencil] to open the **SNMP Details** dialog box.
2. Select one of the following options and enter the appropriate value in the field provided.

You can choose to edit the existing values in the selected SNMP version, or you can select a different SNMP version and enter the desired values.

- Select **SNMP V1/V2C** and specify the community string in the **Community** field.
You can enter “public”, “private”, or a predefined string.

- Select **SNMP V3** and enter the information in the fields provided.
 - a. Enter the SNMP version 3 username in the **Username** field.
 - b. Select the privacy protocol—that is, the encryption standard for the SNMP user—from the **Privacy type** list.
The available options are **AES128**, **DES**, and **None**.
 - c. Enter the password used to generate the key used for encryption in the **Privacy password** field.
The password must be at least eight characters long. You can include all character classes in a password (that is, alphabetic, numeric, and special characters) except control characters.
 - d. Select the authentication type for the SNMP user from the **Privacy type** drop-down list.
The available options are **MD5**, **SHA1**, and **none**.
 - e. Enter the password used to generate the key used for authentication in the **Authentication password** field.
The password must be at least eight characters long. You can include all character classes in a password (that is, alphabetic, numeric, and special characters) except control characters.
- 3. Click **Modify** to save your changes and close the **SNMP Details** dialog box.
The **SNMP Details** section displays the configured SNMP settings.
Alternatively, click **Cancel** to close the dialog box without editing any SNMP probes.

To delete an SNMP probe:

1. Select the SNMP probe that you want to delete in the SNMP Details section and click the **Delete** icon [X].
2. The SNMP probe is removed from the SNMP Details section.

Specifying Credentials

Optionally, specify an administrator name and password to establish the SSH connection for each target device that you configured. If you are using key-based authentication, you do not need to do this step. To specify the credentials:



NOTE: Alternatively, you can select **Device View** from the View selector, click the **Build** icon on the banner, and select **Discover Devices** from the task pane to open the Discovery Profiles window to discover and manage devices.

1. From the View selector, select **Gateway View**. The workspaces that are applicable to this view are displayed.
2. From the Junos Space user interface, click the **Build** icon on the Edge Services Director banner.

The functionalities that you can configure in this mode are displayed in the task pane.

3. From the task pane, select **Services Gateways**.
The Service Gateways page is displayed.
4. Select the **Discover Gateway** option.
5. Click the **Add** icon. The Discovery Profile window appears.
6. Click the **Add** icon in the User Details table. The User Details dialog box is displayed.

A screenshot of the 'User Details' dialog box. It has a blue header bar with the text 'User Details'. Below the header, there are two input fields: 'User Name:' with the text 'user' entered, and 'Password:' with a masked password represented by ten dots. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

7. Specify the administrator username and password, and confirm the password. The name and password must match the name and password configured on the device.
Save the user name and password that you specified by selecting **Save**.

The User Details section of the Discovery Profile window displays the administrator user names that you configured.

Getting Started with Edge Services Director

Based on your network deployment needs and configuration settings, you might require different service types, such as adaptive delivery controller (ADC), traffic load balancer (TLB), stateful firewall (SFW), carrier-grade NAT (CGNAT), and packet filters, to be applied on devices in your topology. It is essential to discover or add the devices that you want to be administered using Edge Services Director to the application database, before you can enable and define services. Also, the devices must be configured with the basic and mandatory device settings, such as routing instances, routing protocols, interfaces, and administrative groups, before they are imported or discovered for additional modifications, such as configuration of services, using the network management application.

The following workflow describes the tasks that you need to perform after the installation of the application to enable effective and streamlined management, provisioning, and troubleshooting of devices and services configured using Edge Services Director.

1. Discover devices using Edge Services Director GUI or the Junos Space Platform workspace. See *Discovering Devices* for instructions on discovering devices from Build mode of Edge Services Director. See *Discovering Devices* in the *Junos Space Network Application Platform User Guide* for instructions on discovering devices using the Junos Space Platform workspace.



NOTE: Before you can add a device using device discovery, the following conditions must be met

- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:


```
set system services ssh protocol-version v2
```
- The NETCONF protocol over SSH is enabled on the device. To enable the NETCONF protocol over SSH on a device, issue the following CLI command:


```
set system services netconf ssh
```
- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices as part of device discovery, ensure that SNMP is enabled on the device with appropriate read-only V1/V2C/V3 credentials.

2. Create a service delivery gateway (SDG) group for a particular domain or zone in your network, or for any logical bundling that is needed. An SDG device can be combined

into a group of devices for easier and streamlined administration. To create SDG groups, see *Creating Service Gateway Groups*.

3. Define key performance indicator (KPI) templates contain the parameters that evaluate the health of a SDG device. The defined KPIs and threshold values enable operators to specify monitoring criteria critical for service operations and administration. A system-created default KPI template is available. This system-created KPI template cannot be edited or deleted. However, an SDG administrator can clone a new template based on this default template. An administrator-created KPI template can be edited or deleted. To clone a KPI template based on an existing, system-defined template, see *Cloning a KPI Template*.
4. Change a managed device to an unmanaged device, or vice-versa, as needed in your network deployment. You can remove the management of such devices from Edge Services Director. For example, in a certain deployment, you might require certain device characteristics to be separately configured without a bulk application of settings. In such a case, you can mark the device as unmanaged, perform the configurations manually using the device CLI interface, and later decide to add it to the managed devices. To work with managed and unmanaged devices, see *Working With Managed Devices* and *Working With Unmanaged Devices*.
5. Use the Object Builder workspace in Edge Services Director to create objects to be used by firewall policies, policy filters, and NAT policies. These objects are stored in the Junos Space database. You can reuse these objects with multiple policies, such as stateful firewall and NAT policies. To import objects into the Edge Services Director database, see *Importing All Types of Objects*.
6. Create service templates, which enables you to configure generic properties and modify it to suit your network deployment needs, thereby enabling streamlined and simplified administration of services (such as stateful firewall [SFW], carrier-grade NAT [CGNAT], application delivery controller [ADC], and traffic load balancing [TLB]) on service delivery gateways (SDGs) in your topology. To create different service templates, see the following:
 - *Creating and Managing ADC Service Templates*
 - *Creating and Managing CGNAT Service Templates*
 - *Creating and Managing SFW Service Templates*
 - *Creating and Managing TLB Service Templates*
7. Create, publish and commission service policy filters, such as packet filters, stateful firewall and NAT policies, on discovered and managed SDGs. A service filter defines packet-filtering (a set of match conditions and a set of actions) for IPv4 or IPv6 traffic. You can apply a service filter to the inbound or outbound traffic at an adaptive services interface to perform packet filtering on traffic before it is accepted for service processing. To work with service policy filters, see the following:
 - *Creating and Managing CGNAT Policy and Filter Instances*
 - *Creating and Managing Packet Filter Policy Instances*
 - *Creating and Managing SFW Policy and Filter Instances*

8. Create service deployment plans to propagate the configuration settings and attributes related to services and policies on the devices. After you create and publish the service templates, you can use these templates to create service deployment plans. When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices. You can create a deployment plan for each of the service planning templates, such as the ones defined for ADC or SFW services, and the policy or filter templates, such as the packet filter or SFW policy, that you have created. A deploy plan contains details about the settings and configuration parameters that must be propagated and provisioned on the SDGs managed by Edge Services Director. To create deployment plans, see *Creating and Assigning a Deployment Plan to Devices*.
9. View transactions associated with deployment plans. A transaction refers to an operation or a task that is performed on the service definitions, configuration parameters, and policy settings that are created for provisioning on the devices or SDGs. A transaction contains a unique identifier that denotes each deployment plan associated with it. Such an automated generation of a transaction for each deploy plan enables you to track, monitor, and maintain a comprehensive record or log of events performed on the devices. To view transactions, see *Viewing Transactions*.
10. Configure and provision filters for packet analysis. The packet analyzer is the endpoint to which the flow collector interface sends traffic for analysis. You can process and export multiple cflowd records with a flow collector interface. To create packet analyzers, see *Creating and Viewing Service Analyzers*.
11. Monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services. Several monitors or widgets are displayed to enable you to track, diagnose, and rectify problems and discrepancies associated with services configured on devices. To evaluate and diagnose the services and device problems using charts and statistical information, see *Understanding Monitor Mode in Edge Services Director*.
12. View information about the health of your network and changing conditions of your equipment. Use Fault mode to find problems with equipment, pinpoint security attacks, or to analyze trends and categories of errors. For example, if you find that a particular device or a service has recorded a large number of critical or major alarms, you can then navigate to the appropriate device settings page or service order page to correct and modify the attributes or diagnose the problems that might be generating the alarms. To view alarms and events, see *Understanding Fault Mode in Edge Services Director*.

Next Steps

After your devices are up and synchronized, much of the function in Edge Services Director is automatically enabled. However, there are a few additional tasks that you will need to perform to use all the features of Edge Services 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 Edge Services 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 Edge Services Director is the feature to diagnose problems with precision and ease. Edge Services 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.

- Set up users

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

You have the ability to set up users with different Edge Services Director privileges. New Edge Services 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 Edge Services Director User Administration](#).

- Learn what you can do with Edge Services Director

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

- Read [Junos Space Edge Services Director Release Notes](#). These release notes highlight the primary features of Edge Services Director.
- Use the extensive help system that guides you through Edge Services 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 Edge Services Director and the different modes and panes in the interface.

Edge Services Director REST API Overview

The Juniper Networks Edge Services Director APIs are based on the Representational State Transfer (REST) standards. REST defines a set of principles for defining Web services, including how a system's resource states are transferred over HTTP. Clients can be written in any language that sends HTTP requests.

You use standard HTTP methods to access the Edge Services Director APIs. For example, HTTP GET is used by a client application to retrieve a resource, get data from a Web server or to execute a query. Common HTTP methods for REST are:

- GET – Retrieve a resource from the server.
- POST – Update a resource on the server.
- PUT – Create a resource state on the server.
- DELETE – Remove a resource state on the server.

Retrieved resources are displayed in human-readable format. Edge Services Director APIs return data in XML or JavaScript Object Notation (JSON).

The following RESTful Web Services are exposed under the Junos Space Edge Services Director root URI:

- Dashboard
- Discovery
- KPI templates
- SDG groups
- Manage devices
- Inventory
- Service Designer
- Monitoring

URI: /api/juniper/sgd

Edge Services Director RESTful Web Services provide programmatic access to the resources that are defined in Junos Space Edge Services Director. Edge Services Director RESTful Web Services follow the same standards and conventions as the Junos Space Network Application Platform RESTful Web Services. The Edge Services Director RESTful Web Services are exposed under the Juniper Networks Junos Space RESTful Web Services root URI (/api). Edge Services Director-related RESTful Web Services are exposed under the /api/juniper/sgd URI.

**Example resource
returned in XML format**

```
<kpiGroupTrendData>
  <kpiNames>kpiName1</kpiNames>
  <kpiNames>kpiName2</kpiNames>
  <trendData>
    <date>2014-04-21T17:41:54.892+05:30</date>
    <values>3</values>
    <values>2</values>
  </trendData>
  <trendData>
    <date>2014-04-21T17:26:54.893+05:30</date>
    <values>3</values>
    <values>2</values>
  </trendData>
  <trendData>
    <date>2014-04-21T17:11:54.893+05:30</date>
    <values>1</values>
    <values>3</values>
  </trendData>
  <trendData>
    <date>2014-04-21T16:56:54.893+05:30</date>
    <values>1</values>
    <values>3</values>
  </trendData>
  <trendData>
    <date>2014-04-21T16:41:54.893+05:30</date>
    <values>2</values>
    <values>3</values>
  </trendData>
  <trendData>
    <date>2014-04-21T16:26:54.893+05:30</date>
    <values>2</values>
    <values>3</values>
  </trendData>
  <trendData>
    <date>2014-04-21T16:11:54.893+05:30</date>
    <values>3</values>
    <values>1</values>
  </trendData>
  <trendData>
    <date>2014-04-21T15:56:54.893+05:30</date>
    <values>3</values>
    <values>1</values>
  </trendData>
  <trendData>
    <date>2014-04-21T15:41:54.893+05:30</date>
    <values>3</values>
    <values>2</values>
  </trendData>
</kpiGroupTrendData>
```

**Example resource
returned in JSON
format**

```
{
  "kpiGroupTrendData":
  {
    "kpiNames":
    [
      "kpiName1",
      "kpiName2"
    ],
    "trendData":
```

```
[
  {
    "date": "2014-04-21T17:44:49.434+05:30",
    "values":
    [
      3,
      2
    ]
  },
  {
    "date": "2014-04-21T17:29:49.434+05:30",
    "values":
    [
      3,
      2
    ]
  },
  {
    "date": "2014-04-21T17:14:49.434+05:30",
    "values":
    [
      1,
      3
    ]
  },
  {
    "date": "2014-04-21T16:59:49.434+05:30",
    "values":
    [
      1,
      3
    ]
  },
  {
    "date": "2014-04-21T16:44:49.434+05:30",
    "values":
    [
      2,
      3
    ]
  },
  {
    "date": "2014-04-21T16:29:49.434+05:30",
    "values":
    [
      2,
      3
    ]
  },
  {
    "date": "2014-04-21T16:14:49.434+05:30",
    "values":
    [
      3,
      1
    ]
  },
  {
    "date": "2014-04-21T15:59:49.434+05:30",
    "values":
    [
```

```

        3,
        1
    ],
    },
    {
        "date": "2014-04-21T15:44:49.434+05:30",
        "values":
        [
            3,
            2
        ]
    }
]
}
}
}

```

Format and Conventions of RESTful Web Services

The media type for the Edge Services Director application must have the following format:

`application/vendor.sgd.service.type+syntax;version=version number` or

`vendor.sgd.service.type+syntax;version=version number`

For example, `application/vnd.net.juniper.space.monitoring.alarmscount+json;version=1`

[Table 3 on page 32](#) describes these parameters.

Table 3: Media parameters

Parameter	Description
vendor	Vendor of the media type. Media types defined by Juniper Networks use vnd.net.juniper. Third-parties must use their own vendor string when they define their own Web services in their applications that are deployed on Junos Space.
service	Name of the Junos Space-specific service. Service names are all lowercase alphanumeric tokens with hyphen separators; for example, device-management, incident-management.
type	Type of resource. Types are all lowercase alphanumeric tokens with hyphen separators; for example, device, incident.
syntax	Representation of the resource, for example xml..
version	Version of the API; versions begin with the numeral 1.

REST standards are well-described in books and on the Internet. It is not the intent of this guide to discuss the RESTful architecture. This document deals with the REST APIs exposed by Edge Services Director.

For information about Junos Space SDK, refer to [Junos Space SDK](#).