



Service Now Getting Started Guide

Release
17.1R1



Modified: 2017-06-07

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

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Service Now Getting Started Guide

17.1R1

Copyright © 2017, 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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Supported Platforms	ix
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Chapter 1	Overview	15
	Automated Support and Prevention Overview	15
Chapter 2	Installing and Configuring Junos Space Network Management Platform	19
	Installing and Configuring a Junos Space Appliance	19
Chapter 3	Installing Junos Space Service Now and Junos Space Service Insight	21
	Installing Junos Space Service Now and Junos Space Service Insight Applications	21
	Uploading a Service Now and Service Insight Image File to a Junos Space Server	21
	Installing Junos Space Service Now and Junos Space Service Insight	23
Chapter 4	Configuring Service Now	25
	Configuring the Operating Mode of Junos Space Service Now	25
	Adding an SNMP Configuration to Service Now	30
	Adding an Organization to Service Now	31
	Adding an End Customer to Service Now Configured in Partner Proxy Mode	34
	Testing Service Now Connection	36
	Creating a Device Group	37
	Installing AI-Scripts on a Device	39
	Adding AI-Scripts Bundle to Service Now	39
	Creating an Event Profile Using an AI-Scripts Bundle	40
	installing the Event Profile on Devices	42
	Creating Notification Policies	44
	Generating Test Cases	46

List of Figures

Chapter 1	Overview	15
	Figure 1: ASAP Solution	17
Chapter 4	Configuring Service Now	25
	Figure 2: Configuring Service Now Operating Mode	26
	Figure 3: Offline Mode	27
	Figure 4: Direct Mode	28
	Figure 5: End Customer Mode	29
	Figure 6: Add Organization Dialog Box	32
	Figure 7: Add Member Dialog Box	35
	Figure 8: Test Connection Result	37
	Figure 9: Create Device Group Page	38
	Figure 10: Add Script Bundle Dialog Box	40
	Figure 11: Add Event Profile Page	41
	Figure 12: Push to Devices Dialog Box	42
	Figure 13: Create Notifications Page	45
	Figure 14: Create an On-demand Incident Status Dialog Box	47

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Chapter 4	Configuring Service Now	25
	Table 3: Description of Fields on the Add Organization Page	32

About the Documentation

- [Documentation and Release Notes on page ix](#)
- [Supported Platforms on page ix](#)
- [Documentation Conventions on page ix](#)
- [Documentation Feedback on page xi](#)
- [Requesting Technical Support on page xii](#)

Documentation and Release Notes

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

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

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

Supported Platforms

For the features described in this document, the following platforms are supported:

- [Junos Space Virtual Appliance](#)
- [JA2500](#)

Documentation Conventions

[Table 1 on page x](#) defines notice icons used in this guide.

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

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

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] <pre> routing-options { static { route default { nexthop address; retain; } } } </pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Overview

- [Automated Support and Prevention Overview on page 15](#)

Automated Support and Prevention Overview

Juniper Networks Automated Support And Prevention (ASAP) is an end-to-end solution designed to streamline operations and enable proactive network management of devices running Junos OS. With ASAP, a network operator can perform the following functions:

- Monitor faults.
- Collect diagnostic data.
- Manage events.
- Create cases for resolving issues.
- Manage inventory.
- Receive notifications from Juniper Support System (JSS) about issues that can affect the device.
- Receive End-of-Life (EOL) and End-of-Service (EOS) notifications from JSS for managed devices and device components.
- Create reports using the received notifications and analyze the impact of known issues on the network.

ASAP is provided to all customers with Juniper Care and Juniper Care Plus service contracts. ASAP comprises the following components:

- Advanced Insight-Scripts (AI-Scripts):

AI-Scripts are XML, XSLT, or SLAX scripts installed on devices running Junos OS Release 11.4 or later to detect events. When an event occurs on a device on which AI-Scripts are installed, AI-Scripts are triggered to collect troubleshooting information from the device, which is bundled in a structured format called a Juniper Message Bundle (JMB).

AI-Scripts generate three types of JMBs—eJMBs, iJMBs, and on-demand JMBs. Event JMBs or eJMBs are generated in response to events occurring on the device. Information JMBs or iJMBs (also known as device snapshots) are generated to provide trending information of a device.

For more information about AI-Scripts, see *AI-Scripts and JMBs Overview*.

- Junos Space Service Now and Junos Space Service Insight applications:
 - Service Now accesses the JMB generated by AI-Scripts from the device, creates an incident for the event in the Service Now database, and notifies the network operator about the event. Service Now can be configured to submit the incident and the associated JMB to JSS automatically to create a case for resolving any issue caused by the event.

You can use Service Now (instead of AI-Scripts) to generate a JMB in situations where you want to check the health of the device well before receiving an iJMB. This JMB is known as an off-box on-demand iJMB. Service Now can also generate off-box on-demand eJMBs and off-box on-demand Return Materials Authorization (RMA) JMBs. Service Now uses the **directive.rc** file to generate the off-box JMBs. The **directive.rc** file in Service Now contains the required commands to generate the JMBs.

For more information about the directive file, see *Directive File Overview*

- Service Insight stores alerts called proactive bug notifications (PBNs) received from JSS and notifies the network operator about impending problems in the network. Service Insight also stores alerts for devices and services nearing EOL, EOS, Last Order Date, or End of Engineering. Service Insight receives these alerts from JSS based on the trending information of iJMBs submitted by Service Now.

You can generate an EOL and PBN report to identify the devices exposed to known issues or bugs and devices nearing EOL or EOS for taking suitable action to mitigate network downtime.

For more information, see *Proactive Information Received from Juniper Support System (JSS)*.

- Juniper Support System (JSS):

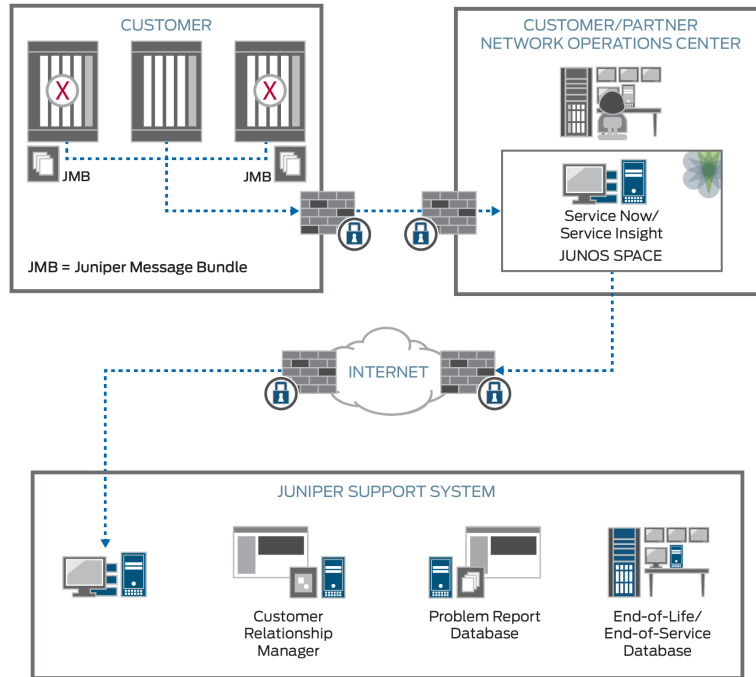
JSS comprises knowledge repositories, such as the EOL or EOS database, the Juniper Customer Relationship Manager (CRM), Juniper Contracts systems, and bugs database.

JSS creates cases for incidents submitted by Service Now. The cases are assigned to JTAC personnel for resolution. Users are notified about the progress of the case through the Service Now GUI.

JSS uses the information present in iJMBs to send alerts about devices and services nearing EOL agreements. While resolving an issue received from a customer, JSS analyzes the nature of the issue and sends PBNs to warn other customers about the issue to mitigate network downtime.

[Figure 1 on page 17](#) represents the ASAP solution.

Figure 1: ASAP Solution



- Related Documentation**
- *AI-Scripts Overview*
 - *Service Now Overview*
 - *Service Insight Overview*

CHAPTER 2

Installing and Configuring Junos Space Network Management Platform

- [Installing and Configuring a Junos Space Appliance on page 19](#)

Installing and Configuring a Junos Space Appliance

Service Automation applications run on the Junos Space Network Management Platform. The Junos Space Network Management Platform is preinstalled in the JA2500 Junos Space Appliance. If you are not using a JA2500 appliance, you can create a Junos Space Virtual Appliance by installing and running the Junos Space Network Management Platform on a virtual machine (VM).

To install the Junos Space Network Management Platform image on a VM to create a Junos Space Virtual Appliance and configure the virtual appliance, see [Junos Space Virtual Appliance Installation and Configuration Guide](#).



NOTE: To install and configure Service Now and Service Insight on a Junos Space Virtual Appliance, we recommend the following size for RAM and partitions of hard disk (for managing about 500 devices):

- RAM: 32 GB
- Hard Disk: 1 TB; partitioned as follows:
 - Minimum 20 GB for /
 - Minimum 20 GB for /tmp
 - Minimum 50G for /var/log
 - Remaining for /var

If you are using a JA2500 appliance, see [JA2500 Junos Space Appliance Hardware Guide](#) for information about installing and configuring the JA2500 Junos Space Appliance.

Related Documentation

- [Installing Junos Space Service Now and Junos Space Service Insight Applications on page 21](#)

- [Configuring the Operating Mode of Junos Space Service Now on page 25](#)

CHAPTER 3

Installing Junos Space Service Now and Junos Space Service Insight

- [Installing Junos Space Service Now and Junos Space Service Insight Applications on page 21](#)

Installing Junos Space Service Now and Junos Space Service Insight Applications

From Junos Space Network Management Platform Release 14.1 onwards, Junos Space Service Now and Junos Space Service Insight are available as hot-pluggable applications. This allows you to install, upgrade, and uninstall Service Now and Service Insight applications independent of the Junos Space Network Management Platform.



CAUTION: If Service Now and Service Insight are already installed on a Junos Space server, do not uninstall them to install or upgrade them to a later version. Uninstalling deletes all the Service Now and Service Insight data from the Junos Space server.

To install Service Now and Service Insight applications, you must first upload the Service Now and Service Insight image to Junos Space Platform.

This topic discusses the following:

- [Uploading a Service Now and Service Insight Image File to a Junos Space Server on page 21](#)
- [Installing Junos Space Service Now and Junos Space Service Insight on page 23](#)

Uploading a Service Now and Service Insight Image File to a Junos Space Server

Before you upgrade or install Service Now and Service Insight, you must upload the required Service Now image file to a Junos Space server.

To upload a Service Now image file to a Junos Space server:

1. Download the Service Now image file from the Juniper Networks support site at <http://www.juniper.net/support/downloads/space.html> to your local file system.
2. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).
3. From the Junos Space Network Management Platform navigation tree, select **Administration > Applications**.

The Applications page appears.

4. On the top-left corner of the Applications page, click the **Add Applications** icon:



The Add Application page appears.

5. On the Add Application page, perform one of the following tasks:

- Upload the Service Now image file by using HTTP.
 - a. Click **Upload via HTTP**.

The Upload Software via HTTP dialog box appears.

- b. Type the name of the Service Now image file or click **Browse** to navigate to the location where the Service Now image file is located on the local file system.
- c. Click **Upload**.



.....
NOTE: Upload the Service Now image file by using SCP if you receive the following message:

File size is too big, use scp to upload this file.
.....

- Upload the Service Now image file by using SCP.

- a. Click the **Upload via SCP** button.

The Upload Software via SCP dialog box appears.

- b. Enter the following details for the image file to be uploaded by using SCP:
 - Username: Enter your username for the local file system.
 - Password: Enter your password for the local file system.
 - Confirm Password: Retype your password.

- Machine IP: Enter the host IP address of the local file system.
- Software File Path: Specify the file path to access the Service Now image file on the local file system.

c. Click **Upload**.

The process of uploading the Service Now image file to the Junos Space server begins and the Upload Application Job Information dialog box appears.

6. In the Upload Application Job Information dialog box, click the *Job ID* link.

The Job Management page is displayed. This page displays the progress of the upload job.

7. After the upload job is complete, go to **Administration > Applications** on the navigation tree to verify the upload.

The Applications page appears.

8. Click the **Add Application** icon.

The Add Application page appears. The uploaded Service Now image file should be listed on this page.

Installing Junos Space Service Now and Junos Space Service Insight

Before you install:

- you must ensure that version of Service Now and Service Insight that you want to install are compatible with the Junos Space Network Management Platform version installed on the Junos Space Server. For information on Junos Space Network Management compatibility, refer to [Junos Space Application Compatibility Matrix](#).

If the installed Network Management Platform version is earlier than the compatible version, upgrade the Network Management Platform to the compatible release first and then upgrade Service Now and Service Insight applications. For information about upgrading Junos Space Network Management Platform, see [Junos Space Software Upgrade FAQ](#).

- upload the Service Now image file to Junos Space server. See “[Uploading a Service Now and Service Insight Image File to a Junos Space Server](#)” on page 21 for information about uploading an image file to the Junos Space server.



CAUTION: If Service Now and Service Insight are already installed on a Junos Space server, do not uninstall them to install another version of Service Now and Service Insight. Uninstalling deletes all the Service Now and Service Insight data from the Junos Space server.


To install Service Now and Service Insight applications:

1. Log in to Junos Space Network Management Platform using the default Username and password (super/juniper123).

2. In the navigation tree, click **Administration > Applications**.

The Applications page appears.

- 3.

On the top-left corner of the Applications page, click the Add Applications icon: .

The Add Application page appears.

4. In the Add Application page, do one of the following:

- If Service Now Release 16.2R1 is listed, select it and click **Install**.
- If the Service Now Release 16.2R1 is not listed, you must upload the release to Junos Space server.

To upload Service Now Release 16.2R1 to Junos Space server, see [“Uploading a Service Now and Service Insight Image File to a Junos Space Server” on page 21](#).

A job is created for the installation process and the Application Management Job Information dialog box appears.

5. In the Application Management Job Information dialog box, click the *Job ID* link. The Job Management page is displayed. This page displays the progress of the upload job.
6. After the installation job is complete, log out of Junos Space and log in to access Service Now. Service Now should be listed in the drop-down menu present above the Junos Space Network Management Platform navigation tree.

Related Documentation

- [Uninstalling Junos Space Service Now and Junos Space Service Insight Applications](#)
- [Junos Space Service Now Global Settings Overview](#)
- [Configuring Global Settings](#)
- [Adding an SNMP Configuration to Service Now on page 30](#)

CHAPTER 4

Configuring Service Now

- [Configuring the Operating Mode of Junos Space Service Now on page 25](#)
- [Adding an SNMP Configuration to Service Now on page 30](#)
- [Adding an Organization to Service Now on page 31](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 34](#)
- [Testing Service Now Connection on page 36](#)
- [Creating a Device Group on page 37](#)
- [Installing AI-Scripts on a Device on page 39](#)
- [Creating Notification Policies on page 44](#)
- [Generating Test Cases on page 46](#)

Configuring the Operating Mode of Junos Space Service Now

The mode in which you can operate Junos Space Service Now depends on your service contract with Juniper Networks. The option to choose the operating mode of Service Now is presented on the Global Settings page of the Service Now Administration workspace, when you access the Service Now GUI for the first time after installing Service Now and Service Insight.

[Figure 2 on page 26](#) Global Settings page with options to configure the mode of operating Service Now.

Figure 2: Configuring Service Now Operating Mode

Global Settings i

Outbound Email Address:

Device Snapshot Purge Time (in days): ▼

Product Health Data Purge Time (in days): ▼

Submitted Incident Purge Time (in days): ▼

Not Submitted Incident Purge Time (in days): ▼

Device Log File Purge Time (in days):

Do not auto submit Incident which are older (in days):

Repeat Incident Dampening Period: ▼

Share Service Now Profile Information

Collect Log Files

Connection Status: **OK**

Direct Mode End Customer Offline Mode

Service Now can be operated in the following modes:

- Demo mode—Service Now operates in demo mode until you create a Service Now organization and validate the organization's connection with JSS.
- Offline mode—Select this mode to operate Service Now in Direct or Partner Proxy modes without having to connect to JSS.
- Direct mode—Select this mode to operate Service Now in Direct or Partner Proxy modes with a connection to JSS.
- End Customer mode—Select this mode to operate Service Now in the End Customer mode.

For information about capabilities of Service Now when operating in various modes, see *Junos Space Service Now Modes*.

To configure the operating mode of Service Now:

1. Log in to the Junos Space GUI.
2. In the Service Now navigation tree, select **Administration > Global Settings**.

The Global Settings page appears. See [Figure 2 on page 26](#).

3. Click one of the modes in which you want to operate Service Now.
 - Offline mode

The Global Settings page for configuring offline mode is shown in [Figure 3 on page 27](#).

Figure 3: Offline Mode

The screenshot shows the 'Global Settings' page with the following configuration:

- Outbound Email Address: servicenow@juniper.net
- Device Snapshot Purge Time (in days): 180
- Product Health Data Purge Time (in days): 30
- Submitted Incident Purge Time (in days): 365
- Not Submitted Incident Purge Time (in days): 365
- Device Log File Purge Time (in days): 30
- Do not auto submit Incident which are older (in days): 10
- Repeat Incident Dampening Period: None
- Share Service Now Profile Information
- Collect Log Files
- Connection Status: OK

At the bottom, the 'Offline Mode' radio button is selected, and there are 'Save', 'Test Connection', and 'Cancel' buttons.

To operate Service Now in offline mode:

- a. On the Global Settings page, click **Offline Mode**.
- b. Click the **Browse** button to browse for the Partner Proxy or the Direct license and click **Upload**.

The license file is imported into Junos Space.



NOTE: The license file is provided to you by Juniper Networks or a qualified Juniper Networks partner.

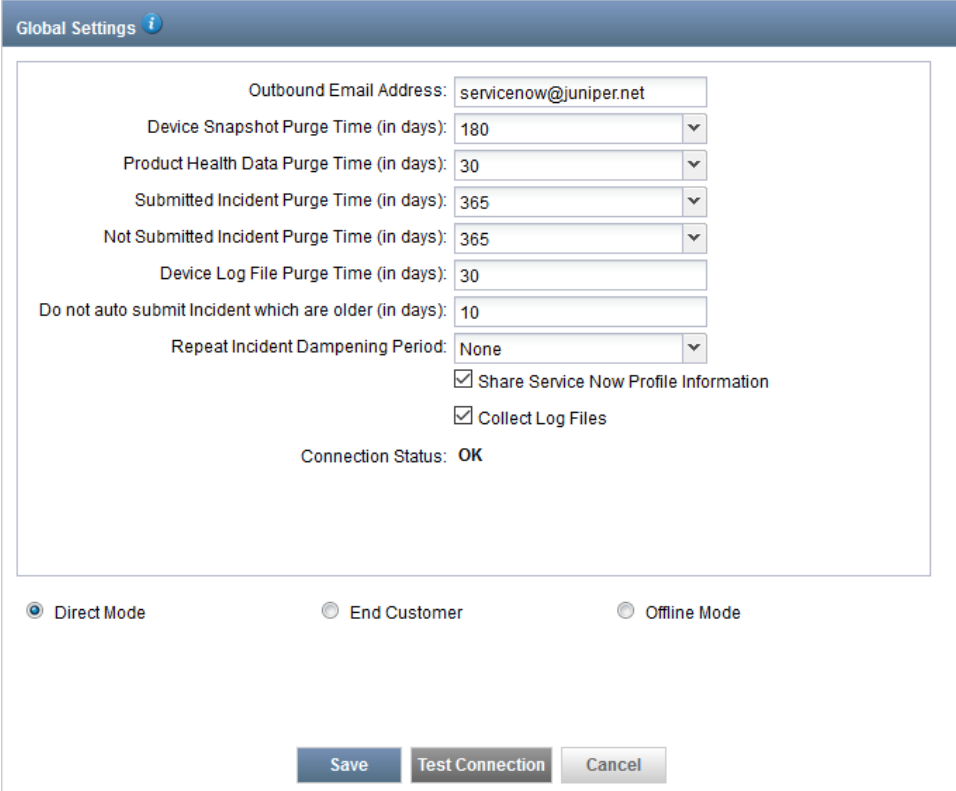
- c. Click **Submit**.

A message indicating that Service Now is successfully configured in the Partner Proxy or Direct mode is displayed.

- Direct mode

This mode is selected by default. [Figure 4 on page 28](#) displays the Global Settings page for configuring Service Now in Direct mode.

Figure 4: Direct Mode



The screenshot shows the 'Global Settings' page for Direct Mode. The page has a blue header with the text 'Global Settings' and an information icon. Below the header is a large white box containing various configuration fields. At the bottom of the page, there are three radio buttons for 'Direct Mode', 'End Customer', and 'Offline Mode', with 'Direct Mode' selected. At the very bottom, there are three buttons: 'Save', 'Test Connection', and 'Cancel'.

Field	Value
Outbound Email Address:	servicenow@juniper.net
Device Snapshot Purge Time (in days):	180
Product Health Data Purge Time (in days):	30
Submitted Incident Purge Time (in days):	365
Not Submitted Incident Purge Time (in days):	365
Device Log File Purge Time (in days):	30
Do not auto submit Incident which are older (in days):	10
Repeat Incident Dampening Period:	None
Share Service Now Profile Information	<input checked="" type="checkbox"/>
Collect Log Files	<input checked="" type="checkbox"/>
Connection Status:	OK

Direct Mode End Customer Offline Mode

Save Test Connection Cancel

To configure Service Now in the Direct mode, click **Submit** and configure organizations using the credentials obtained from Juniper Networks or a qualified Juniper Networks partner. For information about configuring an organization, see [“Adding an Organization to Service Now” on page 31](#).

- End Customer mode

The Global Settings page for configuring Service Now in the End Customer mode is shown in [Figure 5 on page 29](#).

Figure 5: End Customer Mode

Global Settings i

Outbound Email Address:

Device Snapshot Purge Time (in days): ▼

Product Health Data Purge Time (in days): ▼

Submitted Incident Purge Time (in days): ▼

Not Submitted Incident Purge Time (in days): ▼

Device Log File Purge Time (in days):

Do not auto submit Incident which are older (in days):

Repeat Incident Dampening Period: ▼

Share Service Now Profile Information

Collect Log Files

Connection Status: **OK**

Direct Mode End Customer Offline Mode

To configure Service Now to operate in End Customer mode:

- a. On the Global Settings page, click **End Customer**.
- b. In the **Enter IP or Hostname** field, enter the IP address or hostname of the Service Now partner and click **Submit**.
- c. Configure an organization by using the username and password obtained from the Service Now partner. For information about configuring an organization, see [“Adding an Organization to Service Now” on page 31](#).

If the organization is created successfully, a message is displayed indicating that an organization is successfully created and is connected to the Service Now partner. In the Service Now partner, the end customer (referred as connected member) is listed on the Organizations page.

Related Documentation

- [Service Now Modes](#)
- [Adding an Organization to Service Now on page 31](#)
- [Testing Service Now Connection on page 36](#)
- [Adding an SNMP Configuration to Service Now on page 30](#)

Adding an SNMP Configuration to Service Now

You can specify a destination for SNMP traps to be sent when a Service Now notification policy is triggered. SNMP traps are sent to these destination only when the notification policy specifies the SNMP traps to be sent. You can view the SNMP trap destinations on the SNMP Configurations page (**Service Now > Administration > Global Settings > SNMP Configuration**).

To add and manage SNMP servers, you must have Service Now administration privileges.

To add an SNMP server:

1. From the Service Now navigation tree, select **Administration > Global Settings > SNMP Configuration**.

The SNMP Servers page appears.

2. Click **Add**.

The **Add SNMP Server** dialog box appears.



The screenshot shows a dialog box titled "Add SNMP Server" with a close button in the top right corner. The dialog contains the following fields and controls:

- Name:** An empty text input field.
- SNMP Server:** An empty text input field.
- UDP Port:** A text input field containing the value "162".
- Community String:** An empty text input field.
- Protocol Version:** A dropdown menu with "v1" selected.
- Buttons:** "Add" and "Cancel" buttons at the bottom center.

3. Enter a name for the SNMP server. The name must begin with an alphanumeric character. Underscore (`_`), hyphen (`-`) and space are allowed. The maximum number of characters allowed is 64.
4. In the **SNMP Server** field, enter the IP address or hostname of the network management station where Service Now SNMP traps are sent. Do not use special characters.
5. Enter the UDP port number.
The User Datagram Protocol (UDP) port is a mechanism whereby a computer can simultaneously support multiple communication sessions with other computers and programs on the network. A port directs the request to a particular service that can be found at that IP address. The default UDP Port number is 162.
6. Enter a community string using only alphanumeric characters.
A community string is a password that allows access to a network device. It defines the community of people that can access the SNMP information on the device.

7. Select the protocol version from the list that specifies the SNMP versions.
8. Click **Add**.

The specified SNMP server is added to the Service Now database.

Loading MIBs

When using an MIB browser or other SNMP trap receivers such as HP OpenView to monitor the devices with SNMP, the following MIB files must be loaded. The **jnx-smi.mib** file must be loaded first:

1. **jnx-smi.mib**
2. **jnx-ai-manager.mib**

Related Documentation

- *Configuring Global Settings*
- *Editing and Deleting an SNMP Configuration*
- *Managing SNMP Traps*
- *Notification Policies Overview*
- [SNMP MIBs Downloads](#)

Adding an Organization to Service Now

An organization in Service Now represents a unique site ID in the Customer Relationship Manager (CRM) of Juniper Support Systems (JSS). JSS identifies a Service Now application by using the site ID of the organization configured on the Service Now application. An organization is configured on Service Now by providing a site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks for operating Service Now in Direct and Partner Proxy modes. For operating Service Now in End Customer mode, the Service Now partner provides the username and password to configure an organization.

A user should have Service Now administrator privileges to add an organization to Service Now.

To add a Service Now organization:

1. From the Service Now navigation tree, select **Administration > Organizations > Add Organization**.

The **Add Organization** dialog box appears.

Figure 6: Add Organization Dialog Box

The screenshot shows a dialog box titled "Add Organization" with an information icon. It contains the following fields and controls:

- Name:** A text input field.
- Submit Cases as:** A dropdown menu currently showing "Real Cases".
- User Name:** A text input field.
- User Password:** A text input field.
- JMB Filter Level:** A dropdown menu currently showing "Send all information with IP addresses overwritten".
- Buttons:** "Get Sites" (blue), "Submit" (blue), and "Cancel" (grey).

2. Enter the organization parameters in the provided fields. For a detailed description of these fields, see [Table 3 on page 32](#).

Table 3: Description of Fields on the Add Organization Page

Name	Description	Range/Length	Default
Name	Name of the organization	maximum 64 characters are allowed.	
Submit cases as	Specifies if the cases from this organization is to be submitted as real case or test case. The synopsis of a test case sent to JSS is appended with [Test Mode].	The values are: <ul style="list-style-type: none"> • Real cases • Test cases 	Real Cases
User Name	Name used to identify the user in JSS while creating cases, and checking for updates to existing cases. You do not need to enter a username or password if Service Now is in the Offline mode.	128 characters; should be in the e-mail address format. Characters can include alphabets, numbers, and the following special characters: ., -, _ and +.	
User Password	Password for the username required for communicating with JSS or Service Now partner. You do not need to enter a username or password if Service Now is in the Offline mode.	32 characters	

Table 3: Description of Fields on the Add Organization Page (*continued*)

Name	Description	Range/Length	Default
Get Sites (button)	Identifier of the Customer Site in the Customer Relationship Manager(CRM) of JSS. Click Get Sites and select a Site ID from the Site ID list that is generated when you enter the username and password. NOTE: This option is not available when you add an organization in the End Customer mode.	80 characters	
JMB Filter Level	The device configuration information in JMBs to be shared with JSS: <ul style="list-style-type: none"> Do not send Device Snapshots—Does not send device snapshots to JSS Send all information except configuration—Sends all device information except the configuration information Send all information with IP Addresses overwritten—Sends all device information with IP addresses overwritten by asterisks Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information NOTE: The Only send list of features used option is applicable for device snapshots or information JMBs (JMBs) only.	–	Send all information with IP addresses overwritten



NOTE: In the Offline mode, the Add Organization page displays only the Name and the JMB Filter Level fields.

3. Click **Submit**.

This action verifies and saves the organization parameters and returns to the Organization page.

To add a Service Now organization in End Customer mode:

1. From the Service Now navigation tree, select **Administration > Organizations > Add Organization**.

The Add Organization dialog box appears.

2. Enter the organization parameters in the provided fields.

For a detailed description of these fields, see [Table 3 on page 32](#).

3. Click **Submit**.

This action verifies and saves the organization parameters and returns to the Organization page.



NOTE: In End Customer mode, you can add only one organization.

Related Documentation

- [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 34](#)
- [Organizations Overview](#)
- [Junos Space Service Now Global Settings Overview](#)
- [Junos Space Service Now Modes](#)

Adding an End Customer to Service Now Configured in Partner Proxy Mode

Junos Space Service Now that is configured to run in Partner Proxy mode (referred to as Service Now partner) can manage multiple end customers over a secure HTTPS connection. In a Service Now partner, end customers are referred to as connected members. For a Service Now partner to communicate with an end customer, the Service Now application at the end-customer location should be activated in End Customer mode (referred to as Service Now end customer). For information about End Customer mode, see *Service Now Modes*.



NOTE: An end customer can be added to a Service Now partner only after a valid organization is created in the Service Now end customer.

To add an end customer to Service Now configured in Partner Proxy mode:

1. From the Service Now navigation tree, select **Administration > Organization > Add Member**.

The **Add Member** dialog box appears as shown in [Figure 7 on page 35](#).

Figure 7: Add Member Dialog Box

The screenshot shows the 'Add Member' dialog box with the following fields and options:

- Name:** [Text Input Field]
- User Name:** [Text Input Field]
- User Password:** [Text Input Field]
- Confirm User Password:** [Text Input Field]
- JMB Filter Level:** [Dropdown Menu: Send all information with IP addresses overwritten]

Select Configurations Table:

Name	Description
<input type="checkbox"/> Override Address	Select to override the address group associated with end customer devices.
<input type="checkbox"/> Accept BIOS Validations	Select to accept BIOS validations from end customers.
<input checked="" type="checkbox"/> Accept AIS Health Check Incidents	Select to accept AIS Health Check incidents from end customers.

Page 1 of 1 | Displaying 1 - 3 of 3

Submit **Cancel**

2. In the **Name** field, enter a name for the Service now end customer.

The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-). The maximum number of characters allowed is 64.

3. In the **User Name** field, enter a username for the Service Now end customer. The end customer should use this username when submitting cases to the Service Now partner.

The username must be in the `user@example.com` format.

4. In the **User Password** field, enter a password for the username.

5. In the **Confirm User Password** field, enter the same password for confirmation.

6. On the **JMB Filter Level** drop-down menu, select one of the following values to specify the information in a Juniper Message Bundle (JMB) that can be shared with the Service Now partner and Juniper Support System (JSS):

- **Do not send Device Snapshots**—Does not send device snapshots to JSS
- **Send all information except configuration**—Sends all device information in a JMB except the device configuration information
- **Send all information with IP Addresses overwritten**—Sends all the device information; however, the IP addresses associated with the device are overwritten with asterisks (*)
- **Send all information**—Sends all the device information
- **Only send list of features used**—Sends parameters configured without values assigned to the parameters



NOTE: The Only send list of features used option is applicable for device snapshots or information JMBs (iJMBs) only.

7. (Optional) Under **Select Configuration**, do one of the following:

- Select **Override Address** to override address group associated with end-customer devices. Overriding address groups of end customers allows a Service Now partner to send Return Materials Authorization (RMA) incidents of an end customer to JSS using the ship-to address associated with the device by the Service Now partner.
- Select **Accept BIOS Validations** to accept BIOS data from the Service Now end customer for validation.

If you do not select this check box, the **Configure BIOS Validation** option on the Actions menu of Service Now devices is disabled on the Service Now end customer.

- Select **Accept AIS Health Check Incidents** to accept AI-Scripts health check incidents from the Service Now end customer.

8. Click **Submit**.

The end customer is created and displayed on the Organizations page.

Related Documentation

- [Organizations Overview](#)
- [Junos Space Service Now Global Settings Overview](#)
- [Adding an SNMP Configuration to Service Now on page 30](#)

Testing Service Now Connection

After an organization is created, you must test whether or not you are able to connect to JSS or the Service Now partner (in case of end customer).

To test the connection of Service Now with JSS or the Service Now partner:

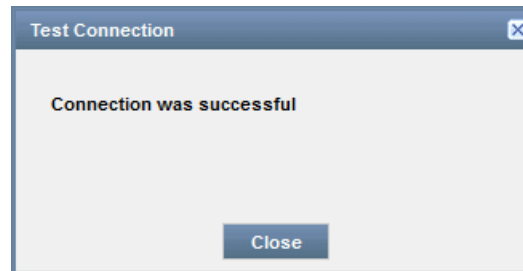
1. From the Service Now navigation tree, select **Administration > Organizations**.

The Organizations page appears.

2. Select the organization whose connection you want to test and select **Check Status** from the Actions menu. Alternatively, right-click the organization and select **Check Status**.

The Test Connection dialog box displays the result of the test connection as shown in [Figure 8 on page 37](#).

Figure 8: Test Connection Result



3. Navigate to **Administration > Global Settings** and confirm that the **Connection Status** displays **OK**.

Service Now is connected to JSS or the Service Now partner.

**Related
Documentation**

- [Creating a Device Group on page 37](#)
- [Device Groups Overview](#)

Creating a Device Group

You can use device groups to group devices within an organization. Only users with Service Now administrator privileges can create device groups and add devices to them. A device added newly to Service Now is assigned to the default device group.

Device Group in Direct mode:

- When a new organization is created, Service Now automatically creates a device group and associates it with the organization.
- You can edit and delete device groups that Service Now creates for the organization.

Device Group in Partner Proxy Mode:

- When a new organization is created, Service Now automatically creates a default device group and associates it with the organization.
- A default device group is generated by Service Now for the first organization created by an end customer.
- Devices added by end customers are automatically added to the default device group.
- Administrators can edit but not delete the default device group for end customers.

To create a device group:

1. From the Service Now navigation tree, select **Administration > Device Groups > Create Device Group**.

The Create Device Group page appears.

Figure 9: Create Device Group Page

2. Enter a name for the device group within the **Name** field.
The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-). The maximum number of characters allowed is 64.
3. In the **Organizations** list, select an organization for this device group.
If you want to associate the device group with a new organization, click **New Organization** and configure an organization. See [“Adding an Organization to Service Now” on page 31](#) for configure an organization.
4. Select the devices that you want to add to this device group from the **Select Device to add them to the Device Group** section.
5. Click **Add**.

The selected devices are added to the device group. To verify if the devices are added, you can view the details of the device group in the Device Groups page.

Related Documentation

- [Device Groups Overview](#)
- [Modifying a Device Group](#)
- [Service Now Devices Overview](#)

- [Installing AI-Scripts on a Device on page 39](#)

Installing AI-Scripts on a Device

AI-Scripts provide the intelligence to a device running Junos OS to detect hardware or software failures.

Junos Space Service Now is shipped with a default AI-Scripts bundle. If needed, you can download other versions of the AI-Scripts bundle from the Juniper Networks website ([AI-Scripts - Download Software](#)) and add them to Service Now.

You must select event scripts from the AI-Scripts bundle to create an event profile and install the event profile on a device running Junos OS. Juniper Message Bundles (JMBs) are generated on the device only for those events that have event scripts included in the event profile.

We recommend that you first identify five of the most common events for which you want JMBs generated and select event scripts only for those events to be installed on the device from the AI-Scripts bundle. This helps you to observe the effect of the AI-Scripts configuration on the device, for example, memory consumed while generating JMBs, the frequency a JMB is generated for an event, performance of the device while JMB is generated, and so on. Install the scripts for other events using a new event profile after your observation.

Before you begin, ensure that you have the following:

- A valid service contract with Juniper Networks
- An user account to access Juniper Networks tools and resources

If you do not have a user account, fill up the registration form at <https://www.juniper.net/registration/Register.jsp> to create a user account.

Installing AI-Scripts on a device involves the following tasks:

- [Adding AI-Scripts Bundle to Service Now on page 39](#)
- [Creating an Event Profile Using an AI-Scripts Bundle on page 40](#)
- [Installing the Event Profile on Devices on page 42](#)

Adding AI-Scripts Bundle to Service Now

To add an AI-Scripts bundle to Service Now:

1. Access [AI-Scripts - Download Software](#).

The AI-Scripts – Download Software page appears.

2. On the AI-Scripts - Download Software page, click the **Software** tab
3. Click the AI-Scripts Install Package of the AI-Scripts release that you want to download. Use the **Version** drop-down list to select an AI-Scripts release version.

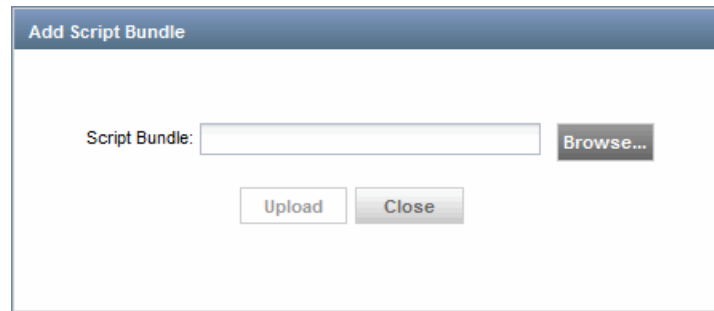
By default, the releases in the latest version are listed on the AI-Scripts - Download Software page.

The LOGIN page appears.

4. Log in to the Juniper Networks authentication system with the username and password provided by Juniper Networks.
5. Click the **AI-Scripts Install Package** link to download the AI-Scripts Install package to your local file system.
6. From the Service Now navigation tree, select **Administration > Event Profiles > Script Bundles > Add Script Bundle**.

The Add Script Bundle page appears as shown in [Figure 10 on page 40](#).

Figure 10: Add Script Bundle Dialog Box



7. Click **Browse**.

The file upload dialog box of your Web browser appears.

8. Locate the AI-Scripts bundle in your local file system and click **Upload**.

The AI-Scripts bundle is uploaded to Service Now and appears on the Script Bundles page.

Creating an Event Profile Using an AI-Scripts Bundle

To create an event profile from an AI-Scripts bundle:

1. From the Junos Space Service Now navigation tree, select **Administration > Event Profiles > Add Event Profile**.

The Add Event Profile page appears as shown in [Figure 11 on page 41](#).

Figure 11: Add Event Profile Page

The screenshot shows the 'Add Event Profile' page. At the top, there is a form with the following fields: 'Profile Name' (containing 'Test Profile'), 'Description' (empty), and 'Script Bundle' (a dropdown menu showing 'jalis-3.7R1.6-signed.tgz' with an 'Add Script Bundle' button next to it). Below the form is a 'Find Events' search box. A 'Show Selected Events' link is located to the right of the search box. The main part of the page is a table with the following columns: 'Event Synopsis', 'Type', 'Sub Type', 'Priority (editable)', 'KB Article', and 'RMA Event'. The table contains several rows of event scripts, each with a checked checkbox in the 'Event Synopsis' column. At the bottom of the page, there are 'Submit' and 'Cancel' buttons.

Event Synopsis	Type	Sub Type	Priority (editable)	KB Article	RMA Event
Category: ACCT (1 Item)					
<input checked="" type="checkbox"/> ACCT_XFER_POOPEN_FAIL	Software Failure	Communication Error	Medium	View KB	No
Category: ALARM (4 Items)					
<input checked="" type="checkbox"/> CONNECTION_SEND_ERROR	Software Failure	Process error	Medium	View KB	No
<input checked="" type="checkbox"/> CONNECTION_RTLOGD_FAIL	Software Failure	Initialization error	Medium	View KB	No
<input checked="" type="checkbox"/> CONNECTION_CRAFTD_FAIL	Software Failure	Initialization error	Medium	View KB	No
<input checked="" type="checkbox"/> CONNECTION_CHASSISD_FAIL	Software Failure	Initialization failure	High	View KB	No
Category: ASP (2 Items)					
<input checked="" type="checkbox"/> ASP_IDS_INV_CLEAR_QUERY_VER	Software Failure	Unexpected output	High	View KB	No
<input checked="" type="checkbox"/> ASP_IDS_INV_CLEAR_QUERY	Software Failure	Unexpected output	High	View KB	No
Category: ASP_L2TP (1 Item)					

2. In the **Profile Name** field, enter a name for the event profile.

The name can contain alphanumeric characters and the Underscore (_), hyphen (-), and space special characters. The maximum number of characters allowed is 255.

3. In the **Description** field, enter a description for the event profile.

The maximum number of characters allowed is 255.

4. From the **Script Bundle** drop-down list, select the AI-Scripts bundle from which you want to select event scripts to be included in the event profile.

5. Select the check box next to Event Synopsis to include all the event scripts present in the selected AI-Scripts bundle, in the event profile.

Alternatively, you can include specific events scripts by selecting the check boxes provided next to the event scripts.

6. (Optional) Click the **Show Selected Events** link to view and verify the event scripts included in the event profile.

7. Click **Submit**.

The Save Event Profile dialog box appears. The dialog box displays a link to apply the event profile to devices manually and another link to return to the Profiles page.

8. Click **Return to the Profiles page** to return to the event profiles page.

After an event profile is created, it can be installed on a device running Junos OS.

installing the Event Profile on Devices

To install event profiles on devices running Junos OS:

1. From the Service Now navigation tree, select **Administration > Event Profiles**.

The event profiles page appears.

2. Select the event profile that you want to install on the devices and select **Push to devices** from the **Actions** menu. Alternatively, right-click the event profile and select **Push to devices**.

The Push to Devices page appears as shown in [Figure 12 on page 42](#).

Figure 12: Push to Devices Dialog Box

Push to Devices

Profile Name: Test_latest
Script Name: jais-4.1R9.4-signed.tgz

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle	Event Profile
Testing-Prod	Default for Testing-Prod	Device1	JN1207242AJA	PTX5000	14.2R4.9		
Testing-Prod	Default for Testing-Prod	Device2	PL0212280006	ACX1100	15.2-20150910_ib_15_2_psd.0		
Testing-Prod	Default for Testing-Prod	Device3	JN11B80B6AEA	M120	14.1R4.8	4.1R9.3	Latest_4_1R9
Testing-Prod	Default for Testing-Prod	Device4	CA1710100208	EX8208	15.1R1.9		
Testing-Prod	Default for Testing-Prod	Device5	AJ3009AA0004	SRX650	12.1X46-D40		
Testing-Prod	Default for Testing-Prod	Device6	462da098-3500-11e5-8a30-00e081ce1bca	QFX3000-G	14.1X53-D17.1		

Page 1 of 1

Never store Script Bundle files on device (if selected roll-back option will not be available)
 Remove Script Bundle files after successful install
 Alter device configuration to enable AI-Script events on device

Notes:
 1) The 'Alter device configuration' option is enabled by default. This option is applicable only for installing AI-Script release versions 5.0 and above. When selected, Service Now pushes the required configuration (if it is not present on the device) and enable the events.
 2) If user does not select the 'Alter device configuration' option, it is expected that user will be pushing the required configuration and enable the events.
 3) When installing AI-Script release version pre-5.0, the 'Alter device configuration' option is not applicable. Service Now will always push the configuration for enabling the events as part of the installation.
 Please refer the KB Article for more details [KB30464](#)

Schedule at a later time

3. Select the devices on which you want to install the event profile.

When the event profile is installed, a copy of the AI-Scripts bundle from which the event profile is created is stored on the device.

4. (Optional) If you do not want to save a copy of the AI-Scripts bundle on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.

By default, this check box is not selected and the AI-Scripts bundle is stored in the device in which it is installed.

5. (Optional) If you want to remove the AI-Scripts bundle from the device after it is installed, select the **Remove Script Bundle files after successful install** check box.

By default, this check box is not selected and the AI-Scripts bundle is stored in the device in which it is installed.

6. (Optional) if you do not want the device configuration to be modified while committing the event profile on the device, clear the Alter device configuration to enable AI-Script events on device check box. By default, this option is selected.



NOTE:

- If you clear the Alter device configuration to enable AI-Script events on device check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device. The static AI-Scripts configuration must be committed on the device manually and the `/var/db/scripts/op/ais-param-set.slax` file executed for AI-Scripts to generate JMBs.
- When you install or upgrade AI scripts releases earlier than Release 5.0 on a device using Service Now Release 15.1 or later, the static AI-Scripts configuration must be pushed manually to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable AI-Script events on device check box is selected or cleared.

7. Click **Submit**.

The Potential Exposure when Event Profile is installed on Devices page appears. An ! icon is placed next to the devices that are susceptible to the events in the event profile.

8. Click **Continue**.

The Install Event Profile dialog box appears. With this dialog box, you can remove devices from the list by clearing their respective check boxes.

9. Click **Install**.

The Job Information dialog box displaying the job ID appears. To view the status of this job, click the job ID link. The Jobs page displays the status of the job.

If you have installed the event profile on a dual Routing Engine, the results displayed on the Jobs page show the status for both the primary Routing Engine and the backup Routing Engine. A Failed status indicates that the installation failed on either of the Routing Engines.

10. Click **OK**.

The View Event Profiles page appears.

Related Documentation

- [Creating Notification Policies on page 44](#)
- [Generating Test Cases on page 46](#)
- [Manually Installing AI-Scripts on Devices](#)

- *Juniper Networks Devices Supported by Service Now and Service Insight*

Creating Notification Policies

You can configure notification policies in Junos Space Service Now to specify when Service Now should send notifications about events occurring on devices in a managed network and the recipients of the notifications. Triggers define instances when a notification should be sent for events. For example, if 'Incident Submitted' notification policy is configured, Service Now sends a notification to recipients whenever an incident is submitted to JSS.

You can further refine the trigger by applying a filter so that notifications are sent only for specific organization, device group, and devices. For example, you can apply a filter to the Incident Submitted trigger so that Service Now sends notifications only when critical incidents from a specific organization are submitted to Juniper Support System (JSS).

You can define the following triggers for notifications to be sent in Service Now:

- **New Incident Detected:** Notification is sent when a new incident is created in Service Now.
- **Incident Submitted:** Notification is sent when an incident is submitted to JSS.
- **Case ID Assigned:** Notification is sent when a case is created for the incident and a case ID is assigned to the case.
- **Case Status Updated:** Notification is sent when the status of the case is updated.
- **New intelligence Update:** Notification is sent when a device snapshot is received by Service Now.
- **Service Contract Expiring:** Notification is sent when the service contract for a device is nearing expiry.
- **New Exposure:** Notification is sent when a proactive bug notification (PBN) is received from JSS.
- **Ship-to Address Missing for Device:** Notification is sent when an RMA incident is submitted to JSS with no ship-to address for a device.
- **Connected Member Device Added/Removed:** Notification is sent when an end customer adds or deletes devices from Service Now organization

To create a notification policy:

1. From the Service Now navigation tree, select **Service Central** > **Notifications** > **Create Notifications**.

The Create Notifications page appears as shown in [Figure 13 on page 45](#),

Figure 13: Create Notifications Page

2. In the **Name** field, enter a notification policy name.

The name must be unique and can contain alphanumeric characters, space, hyphen (-), and underscore (_). The maximum number of characters allowed is 64.

3. From the **Trigger** drop down menu, select a trigger for the notification to be sent.

4. If not already expanded, expand the Apply Filters section and enter the filter parameters.
Different filters are supported for different trigger types.

5. Enter the e-mail IDs of users to whom the notification must be sent.

Use the **Add Email** and **Delete** buttons to add and delete e-mail IDs.

6. In the **Send SNMP Traps to** section, specify the destinations where SNMP traps can be sent when an event occurs.

7. Select the **Send JMB file as attachment in mail** check box if the JMB is to be attached to the notification e-mail.

8. Click **Add**.

The notification policy is created and displayed on the Notifications page.

- Related Documentation**
- [Notification Policies Overview](#)
 - [Generating Test Cases on page 46](#)

Generating Test Cases

To confirm whether incidents are created in Service Now when events occur on a device, generate an on-demand incident on a device and submit a test case to JSS or a Service Now partner (if you are operating Service Now in End Customer mode).

To distinguish a test case, ensure that the Submit Cases attribute of an organization is set to Test Cases.

To generate an on-demand incident:

1. From the Service Now navigation tree, select **Administration > Service Now Devices**.

The Service Now Devices page is displayed.

2. Click a device and select **Create On-demand Incident** from the Actions menu. Alternatively, right-click the device and select **Create On-demand Incident**.

The On-demand Incident dialog box is displayed.

3. Select the **Automatically Submit Case** check box to submit the on-demand incident.

4. Select the **Use Service Now to Generate Incident** check box to generate an on-demand JMB.

5. Select the priority of the incident from the **Priority** list.

The available options are—Critical, High, Medium, and Low. By default, Low is selected.

6. In the **Synopsis** field, enter a synopsis for the on-demand incident.

The maximum number of characters allowed is 155.

7. In the **Problem Description** field, enter a description for the on-demand incident.

The maximum number of characters allowed is 15,000.

8. Click **Submit**.

A Job Information dialog box displaying the job ID appears. You can click the job ID to go to the Create On-demand Incident job on the Jobs page. Double-click the job to open the Create On-demand Incident Status dialog box (Figure 14 on page 47).

Figure 14: Create an On-demand Incident Status Dialog Box

Profile Name	Host Name	Status	Reason
General	ex-4200-sn4	Failed	OP Script execution failed on device 688250. Src File: on-demand.slax Please verify that the AI Script with version 3.2R1 or higher is installed on device. Message from device : Details: Operational RPC Command Results Failed to open netconf channel domainId=0 deviceId=688250

9. Navigate to **Service Central > Incidents**.

The Incidents page appears. If the incident is created successfully, it is listed on the Incidents page.

- Related Documentation**
- *Incidents Overview*
 - *Viewing Incident Details*

