

AI-Scripts, Service Now, and Service Insight Implementation Guide

Published
2019-11-21

Release
18.1R1

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

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

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

AI-Scripts, Service Now, and Service Insight Implementation Guide
18.1R1

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation | ix

Documentation and Release Notes | ix

Documentation Conventions | ix

Documentation Feedback | xii

Requesting Technical Support | xii

Self-Help Online Tools and Resources | xiii

Creating a Service Request with JTAC | xiii

1

Overview

Automated Support and Prevention Overview | 17

Benefits of ASAP | 18

2

Operational Modes

Junos Space Service Now Modes | 23

3

AI-Scripts and JMBs

AI-Scripts and JMBs Overview | 31

AI-Scripts on a Device | 31

Working Modes of AI-Scripts | 33

Type of Events Detected by AI-Scripts | 34

Types of JMBs | 34

Contents of a JMB | 35

Manifest | 36

Trend Data | 43

Attachments | 44

Logs | 46

Generation, Collection, and Processing of a JMB | 47

JMB Generation | 50

JMB Collection | 51

JMB Processing | 52

Junos Space Service Now and Junos Space Service Insight Timers | 54

4

Security and Confidentiality

Security and Confidentiality Overview | 59

Junos Space Network Management Platform Hardening | 60

Ethernet Interfaces | 60

Firewall | 62

Network Policies | 65

TCP Wrappers | 66

Other Hardening Aspects | 66

User Roles and Permissions | 68

Junos Space Service Now Predefined User Roles | 69

Junos Space Service Insight Predefined User Roles | 74

Data Confidentiality in a JMB | 76

Service Now End Customer-Partner Communication Overview | 78

Generating CSR by Service Now Partner | 79

Obtaining Signature of a Certificate Authority | 82

Uploading the Certificate to Service Now Partner | 82

Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate | 82

Obtaining SSL Certificate of the Service Now Partner | 83

Installing the SSL Certificate on a Service Now End Customer | 84

5

Deploying Service AI-Scripts, Service Now, and Service Insight Solution

Deploying AI-Scripts, Service Now, and Service Insight Overview | 89

Installing and Configuring a Junos Space Appliance | 89

Prerequisites for Deploying Junos Space Service Now and Service Insight | 90

Junos Space Platform Requirements | 91

Device Requirements | 91

Determining Device Connections with Junos Space Nodes | 93

Installing Junos Space Service Now and Junos Space Service Insight Applications | 94

Uploading a Service Now and Service Insight Image File to a Junos Space Server | 95

Installing Junos Space Service Now and Junos Space Service Insight | 97

Discovering Devices | 98

Configuring Service Now | 104

Configuring an SMTP Server | 104

Configuring the Operating Mode of Junos Space Service Now | 106

Configuring an Organization | 111

Creating a Connected Member (End Customer) | 113

Testing Service Now Connection | 114

Creating Device Groups | 115

Installing AI-Scripts on a Device | 117

Adding AI-Scripts Bundle to Service Now | 118

Creating an Event Profile Using an AI-Scripts Bundle | 119

installing the Event Profile on Devices | 121

Creating Notification Policies | 123

Generating Test Cases | 125

Service Now and Service Insight Implementation Models | 127

6

Receiving Proactive Information from JSS

Proactive Information Received from Juniper Support Systems (JSS) | 131

PBN, EOL, and EOS Reports Overview | 131

Generating a PBN Report | 131

Generating an EOL Report | 135

7

Troubleshooting

Monitoring AI-Scripts Behavior by Using the AI-Scripts Event Simulator | 141

Troubleshooting Failures While Discovering Devices | 143

Troubleshooting AI-Scripts Installation Issues | 144

Troubleshooting Issues with Generating JMBs | 149

Troubleshooting Issues with Collecting JMBs | 150

Troubleshooting Issues with Creating Incidents | 153

Troubleshooting Issues with Submitting Incidents to JSS or a Service Now Partner | 154

Troubleshooting Issues with Adding an Organization to Junos Space Service Now | 155

Troubleshooting Issues with Receiving Notifications | 157

8

System Log Messages

System Log Messages Used by Junos Space Network Management Platform and Service Now | 161

9

Number of Devices Managed by Service Now

Number of Devices Managed by Service Now | 167

10

Suggested Test Plans

Junos Space Service Now Test Plan | 171

Add an Organization | 171

Discover Devices | 171

Add a Device Group | 172

Add Discovered Devices to Device Group | 172

Install an AI-Scripts Bundle on a Device | 172

Configure Notifications | 172

Generate a Test JMB | 172

Verify Incident Creation in Service Now | 172

Submit the Incident to JSS | 173

Verify whether a Case is Opened for the Incident | 173

Junos Space Service Now Test Plan | 174

Add an Organization | 174

Discover Devices | 174

Add a Device Group | 175

Add Discovered Devices to Device Group | 175

Install an AI-Scripts Bundle on a Device | 175

Configure Notifications | 175

Generate a Test JMB | 175

- Verify Incident Creation in Service Now | 175
- Submit the Incident to JSS | 176
- Verify whether a Case is Opened for the Incident | 176

Junos Space Service Insight Test Plan | 177

- Generate an On-demand Device Snapshot | 177
- Check Whether Device Snapshots are Received by Service Now | 178
- Check Whether Device Snapshots are Uploaded to JSS | 178
- Generate PBN Report | 178
- Generate EOL Report | 179

Appendix

Juniper Networks Devices Supported by Service Now and Service Insight | 183

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | ix
- Documentation Conventions | ix
- Documentation Feedback | xii
- Requesting Technical Support | 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 <https://www.juniper.net/documentation/>.

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

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

Documentation Conventions

Table 1 on page 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>

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

Convention	Description	Examples
<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>
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 <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<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 so that we can improve our documentation. You can use either of the following methods:

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



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

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

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

1

CHAPTER

Overview

Automated Support and Prevention Overview | 17

Automated Support and Prevention Overview

Juniper Networks Automated Support And Prevention (ASAP) is an end-to-end solution designed to automatically resolve product issues, prevent outages, provide insight and increase network productivity. 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 Systems (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 hardware and software events such as fan failure, read-write errors, routing protocol checksum error, critical packet drops, and failure to commit configurations. 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. On-demand JMBs are generated in response to user requests to generate a JMB.

For more information about AI-Scripts, see [“AI-Scripts and JMBs Overview” on page 31](#).

- Junos Space Service Now and Junos Space Service Insight applications:
 - Service Now accesses the JMBs generated by AI-Scripts from devices running Junos OS, 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 is shipped with Service Now and 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 Systems \(JSS\)” on page 131.](#)

- Juniper Support Systems (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.

- Juniper Case Analysis Tool Suite (JCATS)

JCATS is a set of tools that automatically analyze data collected and attached to cases opened in Juniper Networks case management systems and provide analysis results to JTAC engineers. JTAC engineers can use this data to speed up diagnosis and problem resolution.

Benefits of ASAP

- Allows network operators to automatically detect events on a device running Junos OS for early resolution of issues.
- Allows quick collection of necessary troubleshooting data without any manual intervention, thus saving time and effort.
- Provides critical information related to bugs, EOL, and EOS so that network operators and customers can plan to mitigate any adverse impact on their network.

RELATED DOCUMENTATION

AI-Scripts Overview

Service Now Overview

Service Insight Overview

[Installing Junos Space Service Now and Junos Space Service Insight Applications](#) | 94

2

CHAPTER

Operational Modes

[Junos Space Service Now Modes](#) | 23

Junos Space Service Now Modes

Junos Space Service Now collects event and trending data (in the form of Juniper Message Bundles [JMBs]) from devices running Junos OS and submits the data to Juniper Support Systems (JSS) for troubleshooting and analysis. JSS identifies the Service Now application by the organization configured on it. An organization is configured on Service Now with a unique site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks or a qualified Juniper Networks partner (when Service Now is operating in End Customer mode).

Service Now periodically checks and collects JMBs from the managed devices and creates an incident for each JMB collected from the devices. A user can submit an incident manually or configure Service Now to submit an incident automatically to JSS or Service Now partner for creating a case. A case is created in JSS and associated with the site ID of the organization configured on Service Now from which the incident was submitted.

Depending on your contract with Juniper Networks, you can operate Service Now in Direct, End Customer, or Partner Proxy modes. Certain features are enabled or disabled depending on the mode of operation.

- Demo mode—Service Now operates in Demo mode from the time you install Service Now on Junos Space Network Management Platform until you create an organization and validate the organization by establishing a connection with JSS or a Service Now partner.

In Demo mode, you can add one organization and manage up to five devices, manage device inventory, install AI-Scripts on the devices, detect events on the devices, and view JMBs collected from the devices.

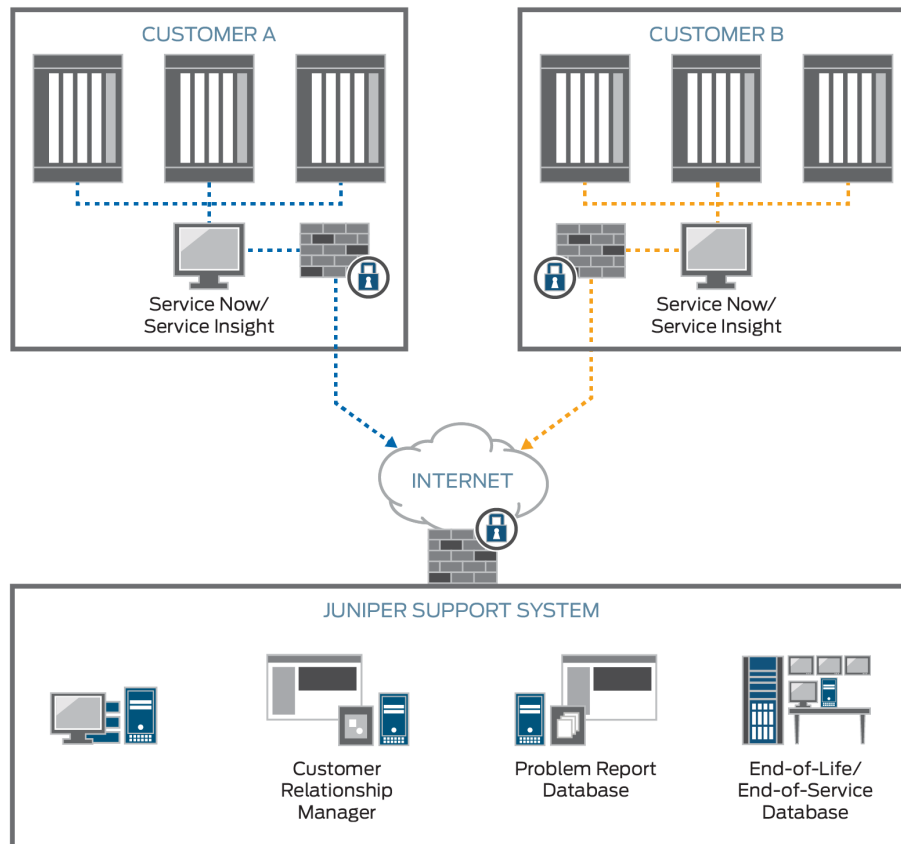
- Offline mode—You can accept a Direct or Partner Proxy license file and activate the Junos Space Platform and Service Now application without having to connect to JSS. You can perform all Service Now tasks except submit incidents, create autosubmit policies, view exposures, or view cases in Case Manager.

NOTE: If Service Now is already in End Customer mode, you cannot operate it in Offline mode.

- Direct mode—In Direct mode, you can add multiple Service Now organizations and devices in Service Now. Service Now is directly connected to JSS, which enables you to submit incidents to JSS and JSS to provide support for the incidents that you submit.

Figure 1 on page 24 shows Service Now operating in Direct mode.

Figure 1: Service Now Operating in Direct Mode



- Partner Proxy mode—A qualified Juniper Networks partner (also known as Service Now partner) can operate Service Now in Partner Proxy mode to manage multiple Service Now end customers (also known as connected members). The Service Now end customers submit incidents to the Service Now partner, who resolves the issues or submits the issues to JSS for resolution.

You can configure multiple organizations and end customers and manage multiple devices in this mode.

- End Customer mode—In End Customer mode, Service Now communicates with JSS through a Service Now partner. When events occur on the devices managed by an end customer, incidents are reported to the Service Now partner. The Service Now partner, if required, submits the incidents to JSS for resolution. The Service Now partner provides the required credentials to an end customer for configuring the Service Now organization. An end customer can be connected to only one Service Now partner.

You can configure only one organization, but can manage multiple devices in this mode.

[Figure 2 on page 25](#) shows Service Now operating in Partner Proxy and End Customer modes.

Figure 2: Service Now Operating in Partner Proxy and End Customer Modes

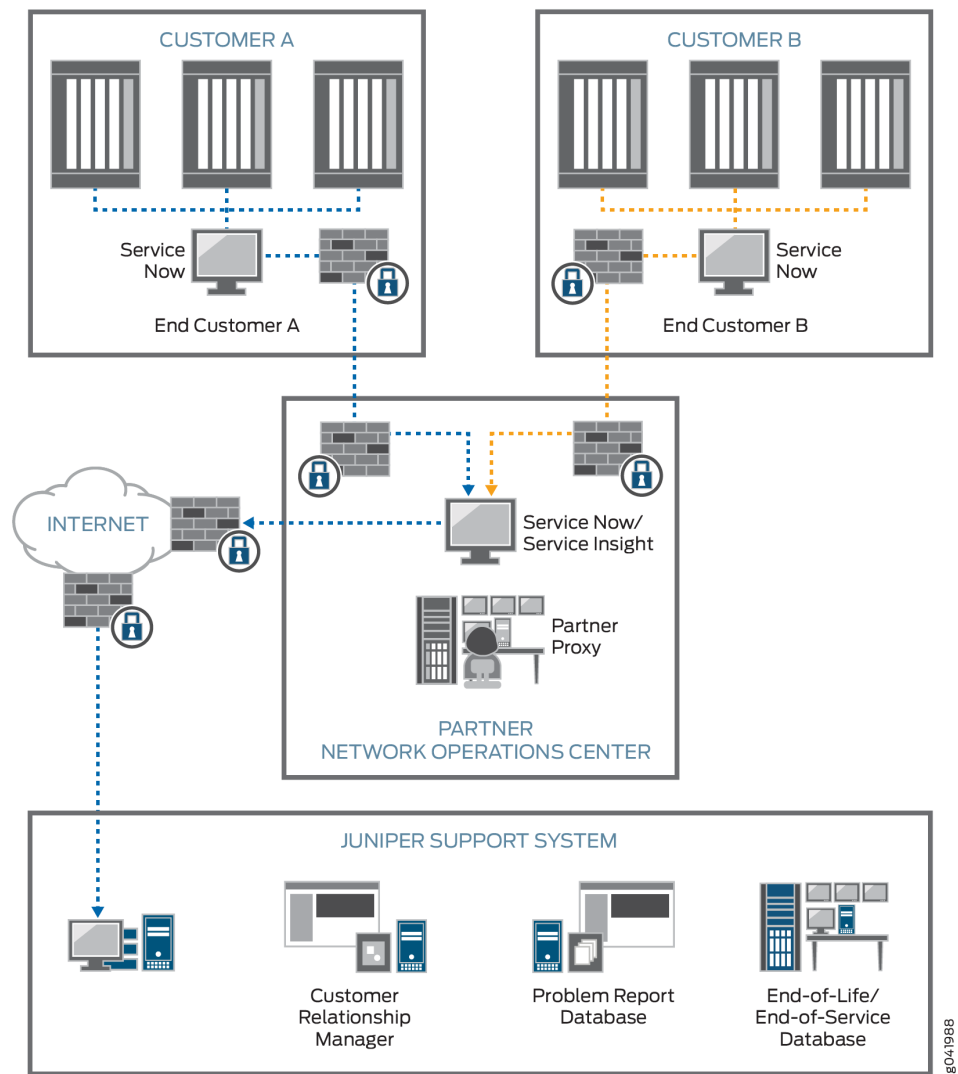


Table 3 on page 25 highlights some of the differences among the various modes of operating Service Now.

Table 3: Features and Tasks Enabled for Service Now Modes

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Number of devices supported	5	Multiple	Multiple	Multiple	Multiple

Table 3: Features and Tasks Enabled for Service Now Modes (continued)

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Number of organizations supported	1	Multiple	Multiple	Multiple	1
Adding connected members	-	-	-	Enabled	-
Updating end-customer cases	-	-	-	Enabled	-
Assigning messages to an end - customer	-	-	-	Enabled	-
Viewing messages assigned to an end - customer	-	-	-	Enabled	-
Submitting incidents for creating technical support cases to JSS	Disabled	-	Enabled	Enabled	Disabled (but can submit incidents to the Service Now partner)
Installing or removing AI-Scripts on or from devices	Enabled	Enabled	Enabled	Enabled (only for devices managed directly by the Service Now partner)	Enabled
Validating the BIOS	Disabled	-	Enabled	Enabled	Enabled
Product Health Data Collection	-	-	Enabled	Enabled	-

Table 3: Features and Tasks Enabled for Service Now Modes (*continued*)

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Other tasks (viewing incidents, configuring notifications, receiving JMBs, managing the inventory, and so on)	Enabled	Enabled	Enabled	Enabled	Enabled

RELATED DOCUMENTATION

[Service Now Administration Workspace Overview](#)

[Service Central Overview](#)

[Configuring Global Settings](#)

[Adding an Organization to Service Now](#)

[Adding an End Customer to Service Now Configured in Partner Proxy Mode](#)

3

CHAPTER

AI-Scripts and JMBs

AI-Scripts and JMBs Overview | 31

Working Modes of AI-Scripts | 33

Type of Events Detected by AI-Scripts | 34

Types of JMBs | 34

Contents of a JMB | 35

Generation, Collection, and Processing of a JMB | 47

Junos Space Service Now and Junos Space Service Insight Timers | 54

AI-Scripts and JMBs Overview

Advanced Insight-Scripts (AI-Scripts) are Extensible Stylesheet Language Transformations (XSLT), Stylesheet Language Alternative Syntax (SLAX), or XML scripts that provide intelligence to devices to automatically detect and report hardware and software failures or other functional abnormalities to network operators so as to ensure maximum network uptime. AI-Scripts are created by experts in Juniper Networks Technical Assistance Center (JTAC) based on the collective experience on troubleshooting devices running Junos OS.

AI-Scripts are imported into Service Now and installed on the devices in the form of AI-Scripts bundles. AI-Scripts bundles contain scripts for individual events. When a particular event occurs, the script for the event in the AI-Scripts bundle is triggered to generate a Juniper Message Bundle (JMB).

A JMB is an XML file containing device information, trend data, system log files, request support information (RSI), and output of Junos OS commands that are executed to obtain information required for troubleshooting the event. A JMB can be an event JMB (eJMB) or informational JMB (iJMB) and contains some or all of the following sections—the Manifest, Trend Data, Attachments, and Logs. For more information about types of JMBs and contents of JMBs, see [“Types of JMBs” on page 34](#) and [“Contents of a JMB” on page 35](#).

AI-Scripts on a Device

The installation of AI-Scripts on a device by using Service Now involves the following steps:

1. Connecting to the device—Service Now uses the NETCONF or Device Management Interface (DMI) channel established while discovering the device to connect with the device.
2. Copying the AI-scripts bundle to the device—Service Now copies the AI-Scripts bundle to the **/var/tmp** folder of the device.
3. Committing the configuration—Service Now commits the **juniper-groups-ais** configuration on the device.
4. Installing the AI-Scripts bundle on the device—The files in an AI-Scripts bundle are installed in the **/var/db/scripts** folder of the device.
5. Committing the event scripts on the device—The files are committed on the device.

On a device running Junos OS, the scripts in the AI-Scripts bundle are installed at the following locations:

- **/var/db/scripts/commit**—Among other commit scripts that are installed from the AI-Scripts bundle, the **jais-SN-activate-scripts.slax** and **jais-activate-scripts.slax** scripts are installed at this location.
 - The **jais-SN-activate-scripts.slax** script is added by Service Now. This file contains a list of events that are relevant to the device and the events that are selected by the user while configuring the event profile.
 - The **jais-activate-scripts.slax** script contains a list of all event scripts in the AI-Scripts bundle and is mainly used for testing purposes.
- **/var/db/scripts/event**—The scripts that are triggered to collect diagnostic and troubleshooting information are installed at this location. The scripts are named after the log message that triggers the script. For example, the **AV_PATTERN_BIG.slax** file is triggered when the AV_PATTERN_BIG message is logged in the system logs of the device.

The **intelligence-event-main.slax** script to generate iJMBs is also installed here.

- **/var/db/scripts/op**—Among other scripts, the following scripts are installed at this location from the AI-Scripts bundle:
 - **on-demand.slax** script: This script is invoked to generate on-demand JMBs.
 - **remove-jais.slax** script: This file helps in the uninstallation and removal of all files from the AI-Scripts bundle installed on the device.
 - **ais-param-set.slax** script: This file contains configuration parameters such as parameters to enable or disable BIOS and request support information (RSI) collection, parameters to define Service Now and Junos Space release to be included in a JMB, and parameters to define an interval to collect BIOS data and generate RSI.
 - **ais-health-report.slax** script: For AI-Scripts Release 4.1R7 and later, this script is used to generate a JMB that provides an insight into the operation of AI-Scripts.
 - **stop-ais-now.slax** script: For AI-Scripts Release 4.1R7 and later, this script is used to temporarily disable JMB generation on a device (for example, while upgrading Junos OS).
 - **ais_event_sim.sh**: This script is used to monitor the behavior of AI-Scripts installed on a device. When you execute this script, an error message is logged in the system log of the device triggering an event script from the AI-Scripts bundle to execute and generate a JMB.

For more information about monitoring AI-Scripts behavior, see [“Monitoring AI-Scripts Behavior by Using the AI-Scripts Event Simulator” on page 141](#).

For information about all the files included in an AI-Scripts bundle, see *Contents of an AI-Scripts Package* in the [AI-Scripts Feature Guide](#).

Refer to the [Service Automation User Guide Addenda - Master List](#) for details about the installation of AI-Scripts on specific platforms.

RELATED DOCUMENTATION

[Installing AI-Scripts on a Device | 117](#)

[Type of Events Detected by AI-Scripts | 34](#)

[Contents of a JMB | 35](#)

[Generation, Collection, and Processing of a JMB | 47](#)

Working Modes of AI-Scripts

AI-Scripts operate in the following modes:

- **Reactive Mode**—In reactive mode, AI-Scripts collect data from the device when a predefined event, such as the failure to allocate memory for a process or failure of a hardware, occurs on the device and store the data at the `/var/tmp` location of the device. Service Now accesses the data from the device for analysis and resolution. The Juniper Message Bundle (JMB) generated in this mode is known as an event JMB or eJMB.
- **Proactive Mode**—In proactive mode, AI-Scripts periodically collect data on vital system functions and store the data at the `/var/tmp` location on the device. This data is accessed by Service Now to monitor the device and to predict and prevent issues that can affect the performance of the device. The JMB generated in this mode is known as an informational JMB, iJMB, or device snapshot.

A user can also trigger the AI-Scripts to generate a JMB. This JMB is known as on-demand JMB or oJMB. When you, as a user, submit an on-demand incident request on a device by using Service Now, Service Now calls the **on-demand.slax** operational script installed on the device from the AI-Scripts bundle to generate an on-demand JMB. An on-demand JMB is a separate type of JMB, but similar to an eJMB. You can use the on-demand option in Service Now to generate JMBs when you do not want to wait for an event to generate a JMB.

Service Now can generate JMBs without using AI-Scripts as well. These JMBs are known as off-box JMBs. You can use Service Now to generate off-box on-demand JMBs when AI-Scripts are not installed on a device.

RELATED DOCUMENTATION

[Juniper Message Bundle Overview](#)

[Exporting a Juniper Message Bundle \(JMB\) to an HTML file](#)

Type of Events Detected by AI-Scripts

AI-Scripts can detect the following types of events on a device:

- Software crashes, software aborts, and SNMP traps
- Failure to allocate memory
- Intrachassis communication message errors (for example, internal socket errors)
- Read/write errors
- Hardware errors (for example, errors related to a chip, memory, temperature, fan, and clock)
- Critical packet drops
- Device overload
- Inconsistencies in the internal data structure
- Routing protocol checksum errors
- Failure to commit configurations

For a complete list of events detected by AI-Scripts, see the [Events Detected by AI-Scripts](#).

RELATED DOCUMENTATION

Types of JMBs

A Juniper Message Bundle (JMB) generated on a device running Junos OS can be of the following types:

- Event JMB or eJMB—JMB generated in response to events such as memory allocation error, read/write errors, or configuration commit failures that occur on devices

An eJMB contains the Manifest, Attachments, and Logs sections.

- Intelligence JMB or iJMB—JMB generated periodically to provide trend and health data of a device

An iJMB contains the Manifest, Trend Data, and Attachments sections.

- RMA JMB—JMB generated when a device component (for example, a fan) fails

When a component fails, the relevant script in the AI-Scripts bundle is triggered to collect the required data for compiling the Return Materials Authorization (RMA) JMB and reporting the event.

An RMA JMB contains the Manifest, Trend Data, and Attachments sections.

- BIOS JMB—JMB generated at predefined intervals to validate the BIOS installed on the device. You cannot view a BIOS JMB.
- On-demand JMB—JMB generated when a user requests that a JMB be generated on the device.

On-demand JMBs can be of the following types:

- On-demand eJMB
- On-demand iJMB
- On-demand RMA JMB

The on-demand JMB is generated by the `/var/db/scripts/on-demand.slax` script installed from the AI-Scripts bundle.

- Off-box JMB—JMB generated on request from a user by using the **directive.rc** file in Service Now. The **directive.rc** file contains commands to generate the JMBs.

Off-box JMBs are usually generated when AI-Scripts are not installed on a device. An off-box JMB can be of the following types:

- Off-box eJMB
- Off-box iJMB
- Off-box RMA JMB

RELATED DOCUMENTATION

Exporting a Juniper Message Bundle (JMB) to an HTML file

Generating an On-Demand Incident

Generating an RMA Incident for a Device

Contents of a JMB

IN THIS SECTION

- Manifest | 36
- Trend Data | 43
- Attachments | 44
- Logs | 46

A Juniper Message Bundle (JMB) is data in a structured format generated by AI-Scripts to provide information for troubleshooting an event that occurred on a device or to provide the trend data of the device. A JMB contains all or some of the following sections:

Manifest

This section of a JMB contains information about the event for which the JMB is generated, the Routing Engine and router on which the event occurred, the core files collected from the router, and the current values of parameters that are configured in AI-Scripts. The information in the Manifest section is used primarily for creating a case in JSS for the event.

[Figure 3 on page 37](#) is a snapshot of the Manifest section of a JMB.

Figure 3: Manifest Section of a JMB

Juniper Message Bundle (JMB)	
Event Information	
Host Event ID:	sn-space-m10i-sys-217-20150409-124642-217
Problem Class:	support
Service Type:	event
Time Occurred:	2015-04-09T12:46:43+05:30
Event Type Group:	Hardware Failure
Event Type:	Environmental problem
Problem Synopsis:	CHASSISD_PSU_TEMPERATURE
Problem Description:	<p>Event message: CHASSISD_PSU_TEMPERATURE</p> <p>Event description: The chassis process (chassisd) detected that the 'temperature check bit' was set in the status bit mask for the indicated power supply unit (PSU). Temperature check bit set for power supply test_pem-slot;</p>
Problem Severity:	4
Problem Priority:	3
KBURL:	http://kb.juniper.net/KB18842
AI Script Version:	4.1R4
Router Information	
Product Name:	m10i
Host Name:	sn-space-m10i-sys
OS Platform:	junos
Routing Engine	
Name:	Routing Engine 0
Mastership State:	Online Master
Routing Engine Software Information	
Component:	
Version:	11.4R7.5
Builder:	

Table 4 on page 37 describes the elements in the Manifest section.

Table 4: Elements in the Manifest Section of a JMB

Element	Description
Event Information	

Table 4: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
Host Event-ID	<p>Specifies the ID of the event in response to which the JMB is generated</p> <p>Host Event-ID is represented in the following format:</p> <p><code><router-name>-<chassis-serial-number>-<YYYYMMDD-HHMMSS>-<sequence number></code>, where:</p> <ul style="list-style-type: none"> • <i>router-name</i> specifies the hostname of the router. • <i>chassis-serial-number</i> specifies the serial number of the router chassis. • <i>YYYYMMDD-HHMMSS</i> specifies the date and time the event occurred on the device. • <i>sequence number</i> varies from 001 through 999 and indicates the sequence of events when multiple events occur at the same time. <p>The <i>sequence number</i> is present only if multiple events occur at the same instance on the device.</p>
Problem Class	<p>Specifies the problem class; the value is always set to Support.</p> <p>This field is used to populate the Problem Class field in the Customer Relationship Management System (CRM) of Juniper Support System (JSS).</p> <p>This field is not applicable for an iJMB.</p>

Table 4: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
Service Type	<p>Specifies whether a JMB is generated as a proactive measure or a reactive measure.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Event: The JMB is generated in response to an event that occurred on the device. (This is a reactive measure.) • Intelligence: The JMB is generated and collected periodically to monitor the vital functions of the device. (This is a proactive measure.) • On-demand: The JMB is generated in response to a request from a user. • Event-RMA: The JMB is generated in response to an Return Material Authorization (RMA) event on the device. This is a reactive measure. • Health-check: The JMB is generated and collected periodically to check the integrity of the BIOS or for any errors related to the AI-Scripts installed on the device. This is a proactive measure.
Time Occurred	Specifies the time at which the event occurred
Event Type Group	<p>Classifies the events that occurred on the device under the following categories:</p> <ul style="list-style-type: none"> • Hardware failure • Software failure • Resource exhaustion <p>This field is not applicable for an iJMB.</p>
Event Type	<p>Specifies the type of event that occurred on the device; for example, MAC error or Process error</p> <p>This field is not applicable for an iJMB.</p>

Table 4: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
Problem Synopsis	<p>Specifies a summary of the event; this field is used to populate the Problem Synopsis field in the CRM.</p> <p>This field can be appended with your text while submitting the incident for resolution to JSS or a Service Now partner.</p> <p>This field is not applicable for an iJMB.</p>
Problem Description	<p>Describes the event; this field is used to populate the Problem Description field in the CRM.</p> <p>This field can be appended with your text while submitting the incident for resolution.</p> <p>This field is not applicable for an iJMB.</p>
Problem Severity	<p>Specifies JTAC's assessment of the impact that the event has on the customer's network</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low <p>This field is not applicable for an iJMB.</p>
Problem Priority	<p>Specifies the customer's perception of the impact that the event has on the network; this field is used to populate the Problem Priority field in the CRM system.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low <p>This field is not applicable for an iJMB.</p>

Table 4: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
KBURL	Specifies the link to the knowledge base (KB) article related to the event This field is not applicable for an iJMB.
AI Script Version	Specifies the version of the AI-Scripts that generated the JMB
Associated Core File	Specifies the core files included in the JMB This field is not applicable for an iJMB.
Router Information	
Product Name	Specifies the name of the product; this field is used to populate the Platform field in CRM.
Host Name	Specifies the hostname assigned to the device
OS Platform	Specifies the routing OS installed on the device
Routing Engine	
Name	Specifies the name of the Routing Engine
Mastership State	Specifies whether the Routing Engine serves as the primary or the backup Routing Engine of the device
Component	Specifies the components of Junos OS such as rpd and chassisid
Version	Version of Junos OS component executing on the Routing Engine
Builder	User who created the Junos OS build
Build Date	Date and time the Junos OS build was created
Service Now Information	

Table 4: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
RSI Collection	Specifies the configuration for collecting Request Support Information (RSI) from the device—whether RSI collection is enabled or disabled and the interval for collecting RSI
BIOS Validation	Specifies whether BIOS validation is enabled or disabled on the device
Log Collection	<p>Specifies whether log collection is enabled or disabled on the device</p> <p>True indicates that log collection is enabled and False indicates that log collection is disabled.</p>
Space Platform Version	Specifies the version of Junos Space Network Management Platform managing the device
Service Insight	Specifies the version of Service Insight installed with Service Now
Service Now	Specifies the version of Service Now managing the device
AI-Scripts Information	
RSI Collection	Specifies the configuration for collecting Request Support Information (RSI) from the device—whether RSI collection is enabled or disabled and the interval for collecting RSI
Log Collection Enabled	<p>Specifies whether log collection is enabled or disabled on the device</p> <p>True indicates that log collection is enabled and False indicates that log collection is disabled.</p>
BIOS Validation	Specifies whether BIOS validation is enabled or disabled on the device
PHD Collection	Specifies whether collection of product health data (PHD) is enabled or disabled on the device. It also states the location of the XML file used by AI-Scripts to determine the CLI commands that are to be run and the time interval during which each command is run.

Table 4: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
PHD Collection Commands File	Specifies the file that contains the commands to collect PHD on the device
JMB Cleanup Interval	Specifies the interval in seconds after which JMBs generated due to PHD collection are deleted

Trend Data

This section of a JMB contains information about hardware and software operating parameters such as CPU and memory utilization of the Routing Engine and traffic statistics of the device. This section is present only in iJMBs.

Trend data is provided for the following components of a device:

- Routing Engine
- Line-card chassis (LCC)
- Switch-card chassis (SCC)
- Flexible PIC Concentrator (FPC)
- Packet Forwarding Engine
- Switch Control Board (SCB)
- Routing protocol process (rpd)
- Kernel

[Figure 6 on page 46](#) shows the Trend Data section of a JMB.

Figure 4: Trend Data Section of a JMB

Juniper Message Bundle (JMB)		
Trend Data Contents		
RPD		
Name	Value	Type a=alphabetic, n=numeric, s=special characters, an=alphanumeric, ns=numericSpecials, ans=alphanumericSpec t=temperature (Unit: C=celsius, F=fahrenheit) m=memory (Unit: B=bytes, K=kilobytes, M=megabytes, G=gigabytes)
task-memory-in-use-size-kB	9126	
task-memory-in-use-avail-percent	0	
task-memory-max-size-kB	9454	
task-memory-max-avail-percent	0	
task-memory-max-when	15/04/18 10:36:25	
task-memory-free-size	2008039	
System		
Name	Value	Type a=alphabetic, n=numeric, s=special characters, an=alphanumeric, ns=numericSpecials, ans=alphanumericSpec t=temperature (Unit: C=celsius, F=fahrenheit) m=memory (Unit: B=bytes, K=kilobytes, M=megabytes, G=gigabytes)
mbufs-in-use-current	656	
mbufs-in-use-cache	1654	
mbufs-in-use-total	2310	
mbuf-clusters-in-use-current	652	
mbuf-clusters-in-use-cache	400	

Attachments

Only files that are relevant to the type of event that triggered the JMB are present in this section. This section provides pointers to the files that contain the output of specific Junos OS commands executed to retrieve specific data pertaining to the event. Some Junos OS commands executed are standard—that is, they are executed for every platform, whereas some are executed for a specific platform.

The following standard Junos OS commands are executed to compile data in this section of the JMB:

- show system processes extensive
- show pfe statistics error
- show system boot-messages
- show system virtual-memory
- show system buffer
- show system queues
- show system statistics
- show task io
- show configuration
- show chassis hardware

NOTE: This command is applicable only on the master Routing Engine.

- request support information

NOTE: This command is dependent on the AI-Scripts parameters governing the collection of the RSI output.

- show system commit
- show system uptime
- file list /var/log/ detail

Figure 5 on page 45 is a snapshot of the Attachments section of a JMB.

Figure 5: Attachments Section of a JMB

Juniper Message Bundle (JMB)					
Attachments details			Click here to download all attachments		
Name	Command	File type	Size (Bytes)	View	Download
bng-fixx1-reg-20150404-093010303_196621_att_ach_shd.xml	show chassis hardware	xml	1526	View	Download
bng-fixx1-reg-20150404-093010306_196621_att_ach_rsi	request support information	text	793761	View	Download
bng-fixx1-reg-20150404-093010308_196621_att_ach_AISESI	multiple	text	55659	View	Download
bng-fixx1-reg-20150404-093010310_196621_att_ach_cfg.xml	show configuration display inheritance	xml	2433	View	Download
bng-fixx1-reg-20150404-093010312_196621_att_ach_ver.xml	show version	xml	702	View	Download
bng-fixx1-reg-20150404-093010314_196621_att_ach_statusmsgs	N/A	text	10859	View	Download

The attachment files are named **host-event-id_attachmentname**, where *host-event-id* specifies the hostname, the *event-id* specifies the date and time the event occurred, and *attachmentname* specifies the type of attachment (for example, cfg, rsi, ver).

The type of JMB determines what attachment files are included in the JMB. For example, an iJMB does not contain the RSI attachment file.

A JMB generally contains the following files as attachments:

- *_AISESI.txt—Contains event support information; output of multiple Junos OS **show** commands

NOTE: This command is dependent on the AI-Scripts parameters governing the collection of the RSI output.

- *_rsi.txt—Contains RSI of the device

NOTE: If this attachment is dampened, the file contains a string that explains the reason.

- *_cfg_xml.xml—Contains device configuration information in XML format
- *_shd_xml.xml—Contains output of the **show chassis hardware** command in XML format
- *_ver_xml.xml—Contains the hostname and version information about the software (including the software help files and AI-Scripts bundle) running on the device
- *_ais_attach_statusmsgs.txt—Displays the status of each JMB attachment generation

You can view or download the attachments using the **View** or **Download** link. The attachments are downloaded in the *.gz format.

Logs

This section of a JMB contains a compressed view of the **/var/log** directory of the device. The log files are retrieved from the device and stored in the Service Now database.

The log files are collected as an attachment if the **/var** directory of the device has more than 20% free space; otherwise, the log files are listed individually and the links to view and download the log files are listed in the JMB.

Figure 6 on page 46 shows the Logs section of a JMB.

Figure 6: Logs Section of a JMB

Juniper Message Bundle (JMB)						
Manifest						
Attachments	Click here to download all logs					
Logs	Logs file details					
	Name	File type	Size (Bytes)	Created	View	Download
	snx-1400- sn1-20150617-002531854_262184_attach_logs_tgz	zip	23087321	2015-06-17 00:25:32	-	Download

RELATED DOCUMENTATION

[Types of JMBs | 34](#)[Generation, Collection, and Processing of a JMB | 47](#)

Generation, Collection, and Processing of a JMB

IN THIS SECTION

- [JMB Generation | 50](#)

- [JMB Collection | 51](#)

- [JMB Processing | 52](#)

Before a device can be managed by Junos Space Network Management Platform, the device must be discovered by Junos Space Platform. After a device is discovered by Junos Space Platform, the following configuration is added to the device:

```
set system syslog file default-log-messages match "<Platform dependent filter>"
set system syslog file default-log-messages any info
set system syslog file default-log-messages structured-data
set snmp trap-group space targets <Space UI VIP>
```

where, *Platform dependent filter* is a platform-dependent match filter, and *Space UI VIP* is the virtual IP address of the Junos Space installation.

After AI-Scripts are installed on the device, the following configuration is added to the device:

```
set groups juniper-ais system scripts commit allow-transients
set groups juniper-ais system scripts commit file jais-activate-scripts.slax optional
set groups juniper-ais system scripts op file ais_change_perm.slax
set groups juniper-ais system scripts op file ais_core_perm.slax
set groups juniper-ais system scripts op file on-demand.slax
set groups juniper-ais system scripts op file remove-jais.slax
set groups juniper-ais system scripts op file ais_arc.slax
set groups juniper-ais system scripts op file ais-attach-file.slax
```

```

set groups juniper-ais system scripts op file stop-ais-now.slax
set groups juniper-ais system scripts op file ais_signalSN.slax
set groups juniper-ais system scripts op file ais_core_chm.slax
set groups juniper-ais system scripts op file ais_all_chm.slax
set groups juniper-ais system scripts op file att_signalSN.slax
set groups juniper-ais system scripts op file ais-rsi-chk.slax
set groups juniper-ais system scripts op file ais-param-set.slax
set groups juniper-ais system scripts op file ais-sleep.slax
set groups juniper-ais system scripts op file ais-error.slax
set groups juniper-ais system scripts op file ais-health-report.slax
set groups juniper-ais system scripts op file ais_xfer_jmb.slax
set groups juniper-ais system scripts op file ais_policy_create.slax
set groups juniper-ais event-options event-script max-datasize 128m
set groups juniper-ais event-options event-script file intelligence-event-main.slax
set groups juniper-ais event-options event-script file bios.slax
set groups juniper-ais event-options event-script file phdc.slax
set groups juniper-ais event-options event-script file Master-event-struct.slax
set groups juniper-ais event-options event-script file Master-event-unstruct.slax
set groups juniper-ais event-options event-script file Master-policy-events.slax
set groups juniper-ais event-options event-script file User-event-struct.slax
set groups juniper-ais event-options event-script file User-event-unstruct.slax
set groups juniper-ais event-options event-script file User-policy-events.slax
set groups juniper-ais event-options event-script file jais-scripts-add.slax
set groups juniper-ais event-options destinations juniper-aim archive-sites /var/tmp/
set apply-groups juniper-ais

```

When an event occurs on a device, the Junos OS running on the device generates the following logs:

- **/var/log/escrpt.log**—The **escrpt.log** file records actions performed by event scripts included in the AI-Scripts bundle.

```

</jmb>Sep 24 15:28:42 end dump
Sep 24 15:28:42 finished event script 'Master-event-struct.slax'
Sep 24 15:28:42 event script processing ends

```

- **/var/log/default-log-messages**—The **default-log-message** file contains information about operations performed on the device—that is, when commits are executed and AI-Scripts have generated data ready for Service Now to collect, and information about other events that is required by Junos Space Platform or connected applications.

```

<13>1 2015-09-24T15:29:07.622-07:00 mx-2 cscript - - - AIS_DATA_AVAILABLE: To be
Transferred : JMB ready for upload /var/tmp/mx-2_15_jmb_ais_prob_20150924_152842
size=19687

```

```
<13>1 2015-09-24T15:31:03.744-07:00 mx-2 cscript - - - AIS_DATA_AVAILABLE: To be
Transferred : All attachments ready for upload
```

- **/var/log/op-script.log**—The **op-script.log** file records actions performed by operational scripts included in the AI-Scripts bundle.

```
Sep 24 15:31:02 op script processing begins
Sep 24 15:31:02 reading op script input details
Sep 24 15:31:02 testing op details
Sep 24 15:31:02 running op script 'att_signalSN.slax'
Sep 24 15:31:02 opening op script '/var/db/scripts/op/att_signalSN.slax'
Sep 24 15:31:02 reading op script 'att_signalSN.slax'
Sep 24 15:31:03 op script output
Sep 24 15:31:03 begin dump
<?xml version="1.0"?>
<op-script-results xmlns:junos="https://xml.juniper.net/junos/*/junos"
xmlns:xnm="https://xml.juniper.net/xnm/1.1/xnm"
xmlns:jcs="https://xml.juniper.net/junos/commit-scripts/1.0"
xmlns:ais="https://xml.juniper.net/ais"/>
Sep 24 15:31:03 end dump
Sep 24 15:31:03 inspecting op output 'att_signalSN.slax'
Sep 24 15:31:03 finished op script 'att_signalSN.slax'
Sep 24 15:31:03 op script processing ends
```

- **/var/log/csscript.log**—The **csscript.log** file records actions performed by the commit scripts included in the AI-Scripts bundle.

```
Oct 5 11:27:10 cscript script processing begins
Oct 5 11:27:10 reading commit script configuration
Oct 5 11:27:10 testing commit script configuration
Oct 5 11:27:10 opening commit script
'/var/db/scripts/commit/jais-activate-scripts.slax'
Oct 5 11:27:10 script file '/var/db/scripts/commit/jais-activate-scripts.slax':
size = 205316 ; md5 = b71a394e7d983a8bf882da9b2993beef sha1 =
b5e94f9c748ceaa8925df32a0ca72c73a597912 sha-256 =
1b9f02cbfc3e93ba5c53e4838c42b6f999ae6c7acdb1bc169f57f2863afcf4da
Oct 5 11:27:10 reading commit script 'jais-activate-scripts.slax'
Oct 5 11:27:10 running commit script 'jais-activate-scripts.slax'
Oct 5 11:27:17 processing commit script 'jais-activate-scripts.slax'
Oct 5 11:27:17 no errors from jais-activate-scripts.slax
Oct 5 11:27:17 saving commit script changes for script jais-activate-scripts.slax
Oct 5 11:27:17 summary of script jais-activate-scripts.slax: changes 0, transients
```

```
2 (allowed), syslog 1
Oct  5 11:27:17 cscript script processing ends
```

- **/var/log/interactive-commands**—The **interactive-commands** file is set up either by Junos OS or manually by a user to record CLI commands that are run on the device to generate a JMB.

```
Sep 24 15:31:20 mx-2 mgd[77367]: UI_AUTH_EVENT: Authenticated user 'root' at
permission level 'super-user'
Sep 24 15:31:20 mx-2 mgd[77367]: UI_LOGIN_EVENT: User 'root' login, class
'super-user' [77367], ssh-connection '192.0.2.100 47460 192.0.2.4 22', client-mode
'cli'
Sep 24 15:31:20 mx-2 mgd[77367]: UI_CMDLINE_READ_LINE: User 'root', command
'xml-mode netconf need-trailer '
Sep 24 15:31:20 mx-2 mgd[77367]: UI_LOGOUT_EVENT: User 'root' logout
Sep 24 15:31:22 mx-2 file[77366]: UI_AUTH_EVENT: Authenticated user 'root' at
permission level 'super-user'
Sep 24 15:31:22 mx-2 file[77366]: UI_LOGIN_EVENT: User 'root' login, class
'super-user' [77366], ssh-connection '192.0.2.100 47460 192.0.2.4 22', client-mode
'netconf'
Sep 24 15:31:22 mx-2 file[77366]: UI_NETCONF_CMD: User 'root' used NETCONF client
to run command 'file-delete
path=/var/tmp/mx-2-15-20150924-152558_ais_attach_logs_tgz'
Sep 24 15:31:22 mx-2 file[77366]: UI_CHILD_START: Starting child '/bin/rm'
Sep 24 15:31:22 mx-2 file[77366]: UI_CHILD_STATUS: Cleanup child '/bin/rm', PID
77368, status 0
Sep 24 15:31:22 mx-2 file[77366]: UI_NETCONF_CMD: User 'root' used NETCONF client
to run command 'close-session'
Sep 24 15:31:22 mx-2 file[77366]: UI_LOGOUT_EVENT: User 'root' logout
```

When an event occurs on a device, the log files inform Junos Space Platform about activities on the device. See the following for information about generation, collection, and processing of JMBs:

JMB Generation

The Junos OS event process (eventd) listens to events generated by Junos OS processes such as chassis process (chassid), routing protocol process (rpd), and device control process (dcd). When an event occurs, the eventd process scans the event table in the kernel and executes the script from the AI-Scripts bundle that matches the event. The eventd process uses criteria such as the name of the event, count of the event, or correlated events occurring within a specific time interval as a trigger to execute the event script.

An event script, when triggered, collects the manifest data for an eJMB or the manifest and trend data for an iJMB and compiles the data into a JMB. AI-Scripts collect attachments and logs separately and store the JMB, attachments, and logs in the **/var/tmp** directory of the device.

JMB Collection

When a JMB is generated and ready for collection, Service Now receives the **AIS_DATA_AVAILABLE: To be Transferred : JMB ready for upload** system log message from the device. The following is a sample of the log message received from an M10i device:

```
AIS_PROCESSING: AI-Scripts Commit script completed
AIS_DATA_AVAILABLE: JMB #1 generation initiated for eventID=998
AIS_PROCESSING: JMB #1 triggered by match with: interval_based_intelligence_event
AIS_DATA_AVAILABLE: WARNING: Cannot update FIFO on rel
AIS_DATA_AVAILABLE: WARNING: Cannot update FIFO on rel
AIS_PROCESSING: JMB #1 is creating the ESI batch file
AIS_PROCESSING: JMB #1 finished attachment:
/var/tmp/M10i-r012-998-20150716-041856_ais_attach_2_cfg_xml size=8481
AIS_PROCESSING: JMB #1 finished attachment:
/var/tmp/M10i-r012-998-20150716-041856_ais_attach_3_shd_xml size=4244
AIS_PROCESSING: JMB #1 finished attachment:
/var/tmp/M10i-r012-998-20150716-041856_ais_attach_4_ver_xml size=9060
AIS_PROCESSING: JMB #1 finished the JMB file
AIS_PROCESSING: Preparing to complete JMB file processing on Master RE
AIS_DATA_AVAILABLE: To be Transferred : JMB ready for upload
/var/tmp/M10i-r012_20150716_042018_998_jmb_ais_intel size=44657
```

In response to the **AIS_DATA_AVAILABLE: To be Transferred : JMB ready for upload** system log message received, Service Now collects the JMB from the device and copies it to the **/var/cache/jboss/SN/Jmb/output** folder of the Junos Space Appliance from where it is copied to the Service Now database. Service Now collects the attachments and log files separately after collecting the manifest and trend data (for iJMBs).

To collect the JMB, Service Now uses the NETCONF over the SSH channel that was created when the device was discovered. For information about the device discovery process, see [“Discovering Devices” on page 98](#).

Service Now starts collecting attachments and logs for a JMB when it receives the **AIS_DATA_AVAILABLE: To be Transferred : All attachments ready for upload** system log message from the device. The following is a sample of the log message received from the M10I device for collecting attachments:

```
AIS_PROCESSING: Starting ESI attachment for JMB #1
AIS_PROCESSING: JMB #1 finished attachment:
/var/tmp/M10i-r012-998-20150716-041856_ais_attach_AISESI size=79200
AIS_PROCESSING: JMB #1 finished attachment:
/var/tmp/M10i-r012-998-20150716-041856_ais_attach_statusmsgs size=1194
AIS_DATA_AVAILABLE: To be Transferred : All attachments ready for upload
```

```
AIS_DATA_AVAILABLE: To be Transferred : Attachment ready for upload
/var/tmp/srx-210h-sn1_998_ais_intel_20150318_082027_ais_atta
ch_5_rsi size=126355
```

After collecting the JMB, attachments or log files Service Now sends the delete remote procedure call (RPC) to the device so that the device can delete files after they are collected.. In response to the delete RPC, the device deletes the specific files from its **/var/tmp** directory.

If, for some reason, Service Now fails to collect the JMB, Service Now attempts to collect the JMB when Service Now receives the next **AIS_DATA_AVAILABLE: To be Transferred : JMB ready for upload** system log message from the device. At each attempt, Service Now collects all JMBs present in the **/var/tmp** folder of a device. Service Now attempts to collect failed attachments once every two hours. See [“Junos Space Service Now and Junos Space Service Insight Timers” on page 54](#) for information about timers that Service Now uses to retrieve data from the device and JSS.

JMB Processing

Service Now creates an incident for each JMB that it receives. You can view the incident and the JMB under the Incidents task of the Service Central workspace of the Service Now GUI. If required, you can manually submit the incident to JSS for creating a case or configure Service Now to automatically submit the incident. A case, when created for the incident, is listed under the View Tech Support Cases task on the Service Now GUI as shown in [Figure 7 on page 53](#).

Figure 7: View Tech Support Cases Page

Applications Service Central > View Tech Support Cases User super logged in Domain: Global Sat Jun 20 2015 04:30 AM IST

Service Now Actions 1 Item Selected

Organization	Site Id	Device Name	Case ID	Device Serial Number	Time Created	Synopsis	Case Type	Priority	Status
TestOrg	99248		2014-0724-0009	CABV4435	Jul 24, 2014 3:24:33 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0002	CABV4435	Aug 3, 2014 7:54:40 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0003	CABV4435	Aug 3, 2014 8:19:23 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0004	CABV4435	Aug 3, 2014 8:19:42 PM IST		Other	2 - High	Open-Reque
TestOrg	99248		2014-0803-0005	CABV4435	Aug 3, 2014 8:28:06 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0006	CABV4435	Aug 3, 2014 10:19:48 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0724-0010	CABV4435	Jul 24, 2014 3:24:43 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0008	CABV4435	Aug 4, 2014 6:33:06 AM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0724-0017	CABV4435	Jul 24, 2014 5:14:07 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0317	CABV4435	Aug 1, 2014 4:42:52 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0318	CABV4435	Aug 1, 2014 4:43:00 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0725-0050	CABV4435	Jul 25, 2014 5:18:08 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0727-0010	CABV4435	Jul 28, 2014 10:15:14 AM IST		Other	2 - High	Open-File Up
TestOrg	99248		2014-0801-0324	CABV4435	Aug 1, 2014 4:46:38 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0323	CABV4435	Aug 1, 2014 4:44:21 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0326	CABV4435	Aug 1, 2014 4:46:57 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0325	CABV4435	Aug 1, 2014 4:46:54 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0070	CABV4435	Aug 1, 2014 1:03:29 PM IST		Other	2 - High	Open-Initial C

Page 1 of 108 Displaying 1 - 30 of 32

A Service Now operating in End Customer mode submits incidents to a Service Now partner. The Service Now partner, if required, submits the end customer's incidents to JSS. The Service Now partner can view cases created for end customer incidents under the View End Customer Cases task on the Service Now GUI.


JSS uses the information contained in the eJMBs to troubleshoot and resolve issues on devices. JSS uses the trend data contained in iJMBs to analyze and provide proactive bug notifications (PBNs) and send alerts to customers about devices and components nearing End of Life (EOL) or End of Service (EOS). Service Insight retrieves the PBNs and EOL and EOS alerts from JSS every midnight. The PBNs and alerts can be viewed in the Insight Central workspace of the Service Insight application.

NOTE: JSS sends PBNs and alerts only to customers with a current Juniper Care or Juniper Care Plus service contract.

You can configure the duration for which an incident and JMB can be stored in the Service Now database on the Global Settings page of the Administration workspace. The incidents and JMBs are automatically deleted from the Service Now database after the specified time lapses.

[Figure 8 on page 54](#) shows a snapshot of the Global Settings page with a purge time configured for device snapshots and incidents.

Figure 8: Global Settings Page

Global Settings 

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**

Note: Please enter the value as '0' in any of the fields above to set the purging interval to 'Never'.

RELATED DOCUMENTATION

[Installing AI-Scripts on a Device](#) | 117

Junos Space Service Now and Junos Space Service Insight Timers

Junos Space Service Now and Junos Space Service Insight use various timers to trigger the retrieval of data from devices running Junos OS and Juniper Support System (JSS). Service Now uses the timers listed

in [Table 5 on page 55](#) and Service Insight uses the timers listed in [Table 6 on page 55](#). The intervals defined for these timers cannot be modified.

Table 5: Timers Used by Service Now

Timer	Description	Interval
Check Case Status	This timer triggers the retrieval of updates to a case submitted to JSS and initiates updates to the status of the case in Service Now.	2 minutes
Get Intelligence Update	This timer triggers the retrieval of intelligence updates from JSS and display of the updates as messages in Service Now.	1 hour
Device Contract Information	This timer triggers the retrieval of device contract information from JSS or a Service Now partner. The device contract information is displayed on the Device Detail page.	1 day
Script Install Advisor (SIA) Information	<p>This timer triggers the retrieval of information about versions of AI-Scripts, Junos OS, and Junos Space Network Management Platform that are susceptible to known issues from JSS.</p> <p>Service Now uses this information to identify the devices that are susceptible to known issues and sets an alert icon next to the identified devices on the Service Now devices page.</p>	1 day
Get iJMB	<p>This timer triggers the retrieval of iJMBs from devices. The iJMBs are displayed on the Device Snapshots page of Service Now.</p> <p>If the device does not generate an iJMB in seven days, Service Now generates and sends an off-box iJMB to JSS.</p>	7 days
JMB Attachment Upload	This timer triggers the retrieval of JMB attachments that might have been missed during JMB collection.	2 hours
JMB and Attachment Retrieval Retry	This timer retries the retrieval of JMBs or attachments if an earlier attempt to retrieve JMBs or attachments failed.	2 hours

Table 6: Timers Used by Service Insight

Timer	Description	Interval
Get EOL Information	<p>This timer triggers the retrieval of information about End of Life (EOL) from the JSS database.</p> <p>Service Insight displays the retrieved information on the Exposure Analyzer page of Service Insight.</p>	The timer is set to retrieve information every midnight (as defined by the NTP configured on the device).

Table 6: Timers Used by Service Insight (continued)

Timer	Description	Interval
Get PBN Information	<p>This timer triggers the retrieval of information about proactive bug notifications from JSS.</p> <p>Service Insight displays the retrieved information on the Exposure Analyzer page of Service Insight.</p>	For Service Now operating in Direct and Partner Proxy modes, the timer is set to retrieve information once every two hours from JSS.

RELATED DOCUMENTATION

[Service Now Incidents Overview](#)
[AI-Scripts Overview](#)
[Service Insight PBN Reports Overview](#)
[Service Insight EOL Reports Overview](#)
[Troubleshooting Issues with Receiving Notifications | 157](#)

4

CHAPTER

Security and Confidentiality

Security and Confidentiality Overview | 59

Junos Space Network Management Platform Hardening | 60

User Roles and Permissions | 68

Data Confidentiality in a JMB | 76

Service Now End Customer–Partner Communication Overview | 78

Installing the SSL Certificate on a Service Now End Customer | 84

Security and Confidentiality Overview

Automated support and prevention (ASAP) provides full data security and confidentiality to customers and partners. Junos Space Service Now and Junos Space Service Insight are implemented on Junos Space Network Management Platform, Service Now and Service Insight use all security mechanisms implemented in Junos Space Platform. See [“Junos Space Network Management Platform Hardening” on page 60](#) for information about security mechanisms implemented in Junos Space Network Management Platform.

Service Automation ensures security and confidentiality by meeting the following requirements:

- Junos Space appliances use SSH and NETCONF or Device Management Interface (DMI) to collect JMBs from a device.
- JMBs are transferred between a Junos Space Appliance and JSS or between a Service Now end customer and Service Now partner through HTTPS connections (port 443).
- A user can access the Service Now and Service Insight GUIs only by using HTTPS (port 443).
- Junos Space appliances initiate all communications with Juniper Support Systems (JSS) by using the eth0 interface. JSS never initiates a connection with Junos Space appliances.
- The level of information in a JMB shared with JSS is configurable; for example, all IP addresses on the device can be hidden in the JMB. See [“Data Confidentiality in a JMB” on page 76](#) for more information.
- Changes made in Junos Space and managed devices are recorded in the audit log database along with details such as the name of the user who initiated the modification, the time of the request, and the Junos Space Appliance that served the modification request.
- AI-Scripts generate JMBs as XML files and store them at the **var/tmp** location of the device. Service Now validates the structure and schema of the JMBs before collecting them from the device.
- A Service Now end customer validates the Service Now partner by using SSL certificates while establishing a connection; see [“Service Now End Customer–Partner Communication Overview” on page 78](#) for an overview of the communication between a Service Now Partner and a Service Now End Customer.

RELATED DOCUMENTATION

[Junos Space Network Management Platform Hardening](#) | 60

[User Roles and Permissions](#) | 68

[Service Now End Customer–Partner Communication Overview](#) | 78

[User Roles and Permissions](#) | 68

Junos Space Network Management Platform Hardening

IN THIS SECTION

- [Ethernet Interfaces | 60](#)
- [Firewall | 62](#)
- [Network Policies | 65](#)
- [TCP Wrappers | 66](#)
- [Other Hardening Aspects | 66](#)

Junos Space Network Management Platform provides network hardening through the following:

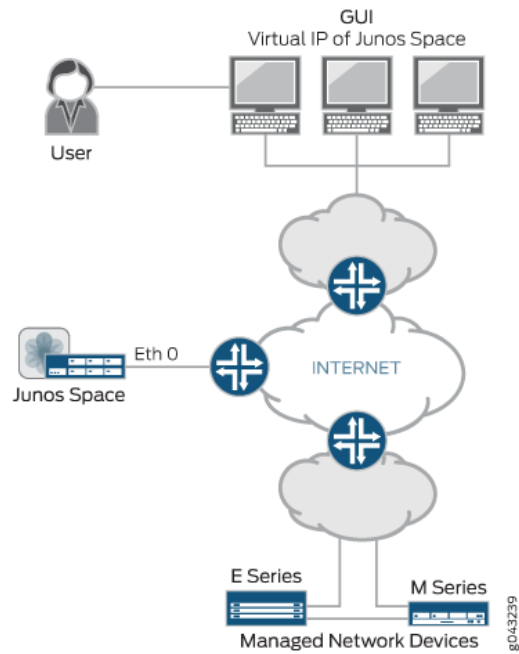
Ethernet Interfaces

A Junos Space Appliance (hardware or virtual) contains four RJ45 10/100/1000 Ethernet interfaces named eth0, eth1, eth2, and eth3.

You can use eth0 and eth3 interfaces for connecting the appliance with managed devices as follows:

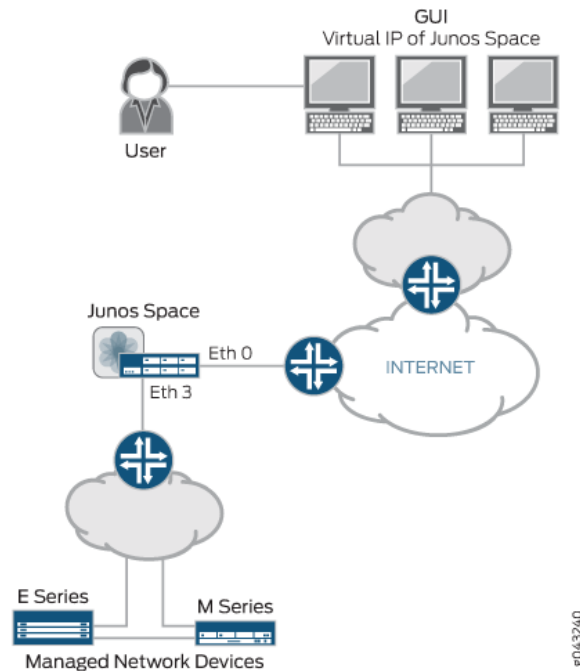
- Use eth0 for all network connectivity of the appliance as shown in [Figure 9 on page 61](#).

Figure 9: Using the eth0 Interface for Connecting Devices



- Use eth0 for connecting with UI clients and other appliances in the same cluster and use eth3 for connecting with managed devices as shown in [Figure 10 on page 62](#).

Figure 10: Using the eth3 Interface for Connecting Devices



The eth1 interface is used to forward the administrative traffic of the Junos Space Appliance. This separates the administrative traffic from the Junos Space GUI traffic and the device management traffic.

Firewall

Junos Space uses the **iptables** utility to control incoming and outgoing network traffic.

The **iptables** utility allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores.

The **jmp-firewall** service (developed by Juniper Networks) controls the iptables firewall. The **jmp-firewall** service is on by default on a Junos Space Appliance. The **Security** option of the Junos Space Settings Menu of the Junos Space Appliance allows you to enable or disable the firewall. For information about enabling Junos Space network settings, see *Changing Network and System Settings for a Junos Space Appliance* for a JA2500 Junos Space Appliance or *Changing Network and System Settings for a Junos Space Virtual Appliance* for a Junos Space Virtual Appliance at [Junos Space Network Management Platform](#).

The following tables list the ports used by Junos Space Platform, Service Now, and Service Insight for communication with Juniper Support System (JSS) and devices:

- [Table 7 on page 63](#)—Ports used by Junos Space Platform
- [Table 8 on page 63](#)—Ports used by Service Now to connect to JSS in Direct mode
- [Table 9 on page 64](#)—Ports used by Service Now to connect to JSS in Partner Proxy mode
- [Table 10 on page 65](#)—Ports used by a Service Now end customer to connect to a Service Now partner
- [Table 11 on page 65](#)—Ports used for administrative access of a Service Now end customer and Service Now partner

Refer to [Junos Space Network Ports](#) for more information.

[Table 7 on page 63](#) lists the ports used by Junos Space Platform.

Table 7: Ports Used by Junos Space Platform

Protocol	Port	Purpose
TCP	7	Inbound to device management IP; used for device discovery
TCP	22	Inbound to the device management IP; used to establish a NETCONF over SSH connection to the router during device discovery
UDP	161	Inbound to the device management IP; used to perform SNMP queries on the device during device discovery
TCP	443	Inbound to the virtual IP (VIP) from external HTTPS clients
TCP	7804	Inbound to the Junos Space server nodes IP; used for devices which use the outbound SSH or device-initiated connection model

[Table 8 on page 63](#) lists the ports used by Service Now to connect to JSS (services.juniper.net) in Direct mode.

Table 8: Ports Used by Service Now to Connect to JSS in Direct Mode

Protocol	Port	Purpose
TCP	443	Outbound connection from Service Now to JSS
UDP	53	(Optional) Outbound from Service Now to DNS for resolution of JSS
TCP	21	FTP control from device to ftp.juniper.net (or a specified FTP server)

Table 8: Ports Used by Service Now to Connect to JSS in Direct Mode (*continued*)

Protocol	Port	Purpose
TCP	20	FTP data transfer from device to ftp.juniper.net (or a specified FTP server) To upload core files from a device to an SFTP server through Service Now to an SFTP server in secure mode, Service Now utilizes existing SSH TCP/22 ports of Junos Space Platform.
TCP	22	Outbound connection from Service Now to sftp.juniper.net (or specified FTP server)

Table 9 on page 64 lists the ports used by Service Now to connect to JSS (services.juniper.net) in Partner Proxy mode.

Table 9: Ports Used by Service Now to Connect to JSS in Partner Proxy Mode

Protocol	Port	Purpose
TCP	443	Inbound to a Service Now partner from Service Now end-customer IP addresses
TCP	443	Outbound from a Service Now partner to JSS
UDP	53	(Optional) Outbound from a Service Now partner to DNS For a direct FTP upload of core files from a device to an FTP server, the device must be connected to the FTP server for the transfer to succeed. In addition, Service Now must have access to the FTP server to create a case-specific directory on behalf of the device before the core file is uploaded.
TCP	21	FTP control from a device to ftp.juniper.net (or the specified FTP server)
TCP	20	FTP data transfer from a device to ftp.juniper.net (or the specified FTP server) To upload core files from a device to an SFTP server through Service Now to an SFTP server in secure mode, Service Now utilizes existing SSH TCP/22 ports of Junos Space Platform.
TCP	22	Outbound from Service Now to sftp.juniper.net (or the specified FTP server)

Table 10 on page 65 lists the ports used by a Service Now end customer to connect to a Service Now partner.

Table 10: Ports Used by a Service Now End Customer to Connect to a Service Now Partner

Protocol	Port	Purpose
TCP	443	Outbound from a Service Now end customer to a Service Now partner IP address
UDP	53	(Optional) Outbound from a Service Now end customer to DNS
TCP	21	FTP control from a device to an FTP server specified by the Service Now partner
TCP	20	FTP data transfer from a managed device to the FTP server specified by the Service Now partner For a secure mode SFTP upload of core files from a managed device through Service Now to an SFTP server, Service Now uses the existing SSH TCP/22 ports specified by Junos Space Platform.
TCP	22	Outbound from Service Now to an SFTP server specified by the Service Now partner

Table 11 on page 65 lists the ports used for administrative access of a Service Now end customer and Service Now partner.

Table 11: Ports Used for Administrative Access of a Service Now End Customer and Service Now Partner

Protocol	Port	Purpose
TCP	443	Inbound for secure HTTPS Web access to the Junos Space GUI
TCP	22	Inbound for secure command-line access to Junos Space
TCP	25	(Optional) Outbound SMTP for delivery of e-mail notifications
UDP	161	(Optional) Inbound SNMP access for remote monitoring of managed devices

Network Policies

The `/etc/sysctl.conf` file controls numerous network policies. Table 12 on page 66 lists some of the important settings that are used to increase network security.

Table 12: Network Policies in the sysctl.conf File

Network Policy	Description
net.ipv4.conf.default.accept_source_route = 0 net.ipv4.conf.all.accept_source_route = 0	Disable source-routed packet acceptance.
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0	Disable ICMP redirect acceptance.
net.ipv4.icmp_echo_ignore_broadcasts = 1	Enable ignore broadcast requests.
net.ipv4.icmp_ignore_bogus_error_responses = 1	Enable bad error message protection.
net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1	Enable RFC-recommended source route validation.
net.ipv4.tcp_syncookies = 1	Enable TCP SYN cookies.

TCP Wrappers

TCP wrappers (tcpd) provide host-based access control system for INET services. The hosts that are allowed access to INET services are configured in the **/etc/hosts.allow** file. The hosts that are denied access to INET services are configured in the **/etc/hosts.deny** file.

Other Hardening Aspects

Other aspects in which the Junos Space Platform is hardened to ensure security and confidentiality are as follows::

- Operating System (OS)Hardening

OS hardening is ensured as follows:

- OS version: Junos Space Network Management Platform Release 14.1 runs on the latest version of CentOS that provides the required security fixes.
- Junos Space access: Access to Junos Space from the console is restricted to only the root user. Non root users must use the **su** and **sudo** commands to run commands remotely on Junos Space.

- **Default file permissions:** The default UNMASK for a file is set to 0027. We recommend that you do not modify the default UNMASK.
- **Disk Partitions:** The file system is partitioned into `/root`, `/var`, `/var/log`, and `/tmp` to offer greater granularity for permissions.
- **Login attempts:** The `pam_tally2` module is configured to lock a user account after three unsuccessful log in attempts. The lock is retained for 20 minutes.
- **Bash shell:** The bash shell is configured to automatically log out idle users. You can modify the settings in the `/etc/ssh/sshd_config` file.
- **Log rotation:** Junos Space has log rotation enabled for the following to avoid filling up of the disk space with logs or making the logs large—`/var/log/messages`, `/var/log/boot`, `/var/log/secure`, and `/var/log/maillog`.

- **Database Hardening:**

Database hardening is ensured as follows:

- Junos Space uses MySQL as its database. To make the database secure, in Junos Space Release 13.3 and later, it has been made mandatory even for the admin user to provide a password to obtain access to the MySQL database. We recommend that the password for the super user account (root) in MySQL be changed as follows:

```
mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('newpass');
mysql> SET PASSWORD FOR 'root'@'hostname' = PASSWORD('newpass');
mysql> COMMIT
```

where *hostname* is the name of the host and *newpass* is the new password.

- The file privileges to the directories in the database are restricted to read and write.
 - The mysql daemon is configured to run in the chroot jail environment.
- **Secure Shell (SSH) Daemon Hardening**
The SSH daemon is hardened as follows:
 - **Linux system accounts:** Junos Space provides a number of user accounts such as root, ntp, postgres, apache, and so on. The `/etc/passwd` file contains details of the account. We recommend that the user accounts that are not required be deleted.
 - **Shared key authentication:** Junos Space provides the option for shared key authentication to improve security by restricting SSH access to only those systems that know the shared key. For information about shared key authentication, see [Key-Based Authentication Overview](#).
 - **Limit network access:** The SSH daemon is limited to listen to connections on only internal interfaces. The interfaces that can listen to the SSH daemon are defined in the `/etc/ssh/sshd_config` file.
 - **Web Server Hardening**

The Web server is hardened as follows:

- Junos Space uses only the GET, POST, PUT and DELETE methods. All other HTTP methods are deactivated.
- The display of server version information on HTTP headers is disabled.
- The index option is disabled to avoid listing the files and directories in the root directory of a file.
- The HTTP trace option is disabled.
- The Web service is restricted to listen to connections on internal interfaces only.
- You can provide an additional layer of security to Junos Space by using SSL certificates.

For information about SSL certificates, see [Certificate Management Overview](#) and [Installing Custom SSL Certificate on Junos Space Server](#).

RELATED DOCUMENTATION

[Security and Confidentiality Overview | 59](#)

[Junos Space Ethernet Interfaces Overview](#)

User Roles and Permissions

IN THIS SECTION

- [Junos Space Service Now Predefined User Roles | 69](#)
- [Junos Space Service Insight Predefined User Roles | 74](#)

Junos Space Network Management Platform provides role-based access control (RBAC). A user is allowed access to the Junos Space Network Management Platform and applications after authentication and authorization.

A Junos Space Super Administrator or User Administrator controls the workspaces that users can access, the system resources that a user can view and manage, and the tasks available to users within a workspace. RBAC is enforced in the Junos Space user interface navigation hierarchy by workspace, task group, and task. A user can access only those portions of the navigation hierarchy that are explicitly granted through access privileges. For more information about role-based access control, see the *Role-Based Access Control Overview* topic of the *Junos Space Network Management Platform User Guide* at [Junos Space Documentation](#).

While Junos Space Platform allows creating users with custom permissions, it also has a set of predefined user roles. These predefined roles cannot be modified or deleted.

For information about predefined user roles in Junos Space Platform, see the *Predefined Roles Overview* topic of the *Junos Space Network Management Platform User Guide* at [junos Space Documentation](#). For information about predefined user roles for Junos Space Service Now and Junos Space Service Insight, see the following:

Junos Space Service Now Predefined User Roles

[Table 13 on page 70](#) lists the predefined roles and associated tasks permitted in Service Central and Administration workspaces of Junos Space Service Now.

Table 13: Predefined Roles for the Service Now Application

Role	Workspace	Task Groups and Tasks
Service Now Admin	Administration	

Table 13: Predefined Roles for the Service Now Application (continued)

Role	Workspace	Task Groups and Tasks
		<ul style="list-style-type: none"> ● Incident Filters: Create basic filter, create advanced filter, import incident filters, modify incident filters, delete incident filters, export incident filters, reorder incident filters, enable incident filters, disable incident filters, and assign incident filters to a domain ● Auto Submit Filters: Create basic filter, create advanced filter, import auto submit filters, modify auto submit filters, delete auto submit filters, export auto submit filters, reorder auto submit filters, enable auto submit filters, disable auto submit filters, and assign auto submit filters to a domain ● Global Settings: Manage directive file, configure an FTP server for uploading core files, manage SNMP traps, and configure Service Now partner certificates on a Service Now end customer, configure advanced settings ● Address Group: Create address groups, associate address groups with devices, modify address groups, delete address groups, and assign address groups to domains ● Device Groups: Create device groups, modify device groups, set a device group as the default device group, associate address groups with device groups, assign device groups to domains, and delete device groups from Service Now ● Service Now Devices: Add devices to Service Now, export device inventory information, associate devices with autosubmit policies, associate devices with device groups, check FTP server configuration, configure RSI and log file collection on devices, create on-demand incidents, associate devices with address groups, export device information, install event profiles on devices, request Return Materials Authorisation (RMA), uninstall event profile from devices, view exposure of devices to known events, view incidents generated on Service Now, assign the Service Now devices to domains, and delete devices from Service Now ● Email Templates: Modify default content of an Email template and restore the modified content of an Email template to its default content ● Event Profiles: Add AI-Scripts bundles to Service Now, set an AI-Scripts bundle as the default AI-Scripts bundle in Service Now, delete AI-Script bundles, create event profiles, import event profiles, export event profiles to an XML file, push event profiles to devices, clone event profiles, set an event profile as the default profile, view events included in event profiles, view devices associated with event profiles, assign event profiles to domains, and delete event profiles from Service Now ● Auto Submit Policy: Create autosubmit policies, export incident reports, modify autosubmit policies, change the dampening status of autosubmit policies, assign autosubmit policies to a domain, and delete autosubmit policies from Service Now ● Organization: Add an organization to Service Now, add end customers to

Table 13: Predefined Roles for the Service Now Application (continued)

Role	Workspace	Task Groups and Tasks
		<p>organizations, check the connection status of Service Now with Juniper Support System (JSS) or with a Service Now partner, modify organizations, associate address groups with organizations, delete organizations, update core file upload configuration, view information messages received from JSS, and assign organizations to domains</p> <ul style="list-style-type: none"> ● Product Health Data Collection (PHDC): Configure PHDC, modify PHDC, delete PHDC, enable PHDC on devices, disable PHDC on devices, reschedule PHDC on devices, retry PHDC on failed devices, abort PHDC on devices, delete product health data (PHD) files, download product health data files, export information about product health data and devices
	Service Central	<ul style="list-style-type: none"> ● Incidents: Create autosubmit policies, view end-customer cases in Case Manager, update end-customer cases, export JMB to HTML, export incident summaries to Excel, assign an owner to incidents, view end-customer cases created in Service Now, flag incidents to users, submit cases to JSS or a Service Now partner, view KB articles related to an incident, delete incidents, view tech support cases in Case Manager, update tech support cases, upload core files to JSS, Upload attachments to cases, and view JMB associated with an incident ● Information: View iJMBs, export iJMBs to HTML, delete iJMBs, assign messages received from JSS to connected members, assign ownership to messages, delete messages, Flag messages to users, and scan devices for impact based on messages received from JSS ● View Tech Support Cases: View cases in Case Manager, update cases, and upload text or binary attachments to cases ● View End Customer Cases: View end-customer cases in Case Manager and Update end-customer cases ● Device Analysis: Delete BIOS validations, export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files ● JMB Errors: Download error JMBs and delete error JMBs ● Suppressed Events: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs ● Notifications: Create notifications, edit notification filters and actions, copy notifications, delete notifications, enable or disable notifications, and assign notifications to domains

Table 13: Predefined Roles for the Service Now Application (continued)

Role	Workspace	Task Groups and Tasks
Service Now Read Only	Administration	Service Now Devices: Export event profiles, export devices, view exposure of devices to known events, and create on-demand device snapshots, export information about product health data and devices, download product health data files
	Service Central	<ul style="list-style-type: none"> • Incidents: Export a JMB in HTML format, view JMBs, export incident summary to Excel, and view tech support and end-customer cases in Case Manager • JMB Errors: Download error JMBs • Tech Support cases: View tech support cases in Case Manager and update cases • Information: View iJMBs, export iJMBs to HTML and scan devices for impact based on messages received from JSS • Device Analysis: Export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • Suppressed Events: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • Notifications: Create notifications • End-customer cases: View end-customer cases in Case Manager

Table 13: Predefined Roles for the Service Now Application (*continued*)

Role	Workspace	Task Groups and Tasks
Service Now Unrestricted User	Administration	Service Now Devices: Export devices, view exposure of devices to known events, create on-demand device snapshots, and export event profiles, export information about product health data and devices, download product health data files
	Service Central	<ul style="list-style-type: none"> • Incidents: Export JMBs to HTML, view JMBs, export incident summaries to Excel, view tech support and end-customer cases in Case Manager, update tech support and end-customer cases, delete incidents, submit cases to JSS, assign ownership to incidents, and flag incidents to users • Tech Support cases: View tech support cases in Case Manager and update cases • JMB Errors: Download error JMBs and delete error JMBs from Service Now • Suppressed Events: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • View Tech Support Cases: View tech support cases in case manager, update cases in case manager • Information: Assign owners to messages received from JSS, flag messages received from JSS to users, delete messages received from JSS, assign messages received from JSS to end customers, export iJMBs to HTML, view iJMBs, and delete iJMBs from Service Now • Device Analysis: Delete BIOS validations, export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • View End Customer Cases: View end-customer cases in Case Manager and update end-customer cases • Notifications: Create notifications, edit filters and notifications, copy notifications, enable or disable notifications, assign notifications to domains, and delete notifications

Junos Space Service Insight Predefined User Roles

Table 14 on page 75 lists the predefined roles and associated tasks permitted in the Insight Central workspace of Junos Space Service Insight.

Table 14: Predefined Roles for the Service Insight Application

Role	Task Groups and Tasks
Service Insight Administrator	<ul style="list-style-type: none"> • Exposure Analyzer: View PBNs that can impact devices, generate EOL reports, and generate PBN reports • EOL Reports: Regenerate EOL reports, export EOL reports, and delete EOL reports from Service Insight • PBN Reports: Regenerate PBN reports, export PBN reports, and delete PBN reports • Targeted PBNs: Scan for impact, flag PBNs to users, e-mail PBN to users, assign owners to PBNs, and delete PBNs from Service Insight • Notifications: Create notifications, edit filters and actions in notifications, copy notifications, delete notifications, enable or disable notifications, and assign notifications to domains
Service Insight Read Only User	<ul style="list-style-type: none"> • Exposure Analyzer: View PBNs that can impact devices • EOL Reports: Export EOL reports in Excel format • PBN Reports: Export PBN reports in Excel format • Targeted PBNs: Scan devices for that are impacted by the PBNs
Service Insight Unrestricted User	<ul style="list-style-type: none"> • Exposure Analyzer: View PBNs that can impact devices, generate EOL reports, and generate PBN reports • EOL Reports: Regenerate EOL reports, export EOL reports, and delete EOL reports • PBN Reports: Regenerate PBN reports, export PBN reports, and delete PBN reports • Targeted PBNs: Scan for impact, flag PBNs to users, e-mail PBNs to users, assign owners to PBNs, and delete PBNs from Service Insight • Notifications: Create notifications, edit filters and actions in notifications, copy notifications, delete notifications from Service Insight, enable or disable notifications, and assign notifications to domains

RELATED DOCUMENTATION

[Insight Central Overview](#)

[Service Central Overview](#)

Data Confidentiality in a JMB

Junos Space Service Now collects data from a device and submits the data to JSS. To ensure security while collecting JMBs, attachments, or log files from a device, Service Now uses the HTTPS or SCP protocol to submit the JMBs, attachments, or log files to JSS or a Service Now partner.

Service Now provides export options to view data in a JMB that is being shared with JSS or a Service Now partner and various filters to set the level of device data in a JMB that can be shared. This filter is configurable for each organization added to Service Now. The following filters can be configured:

- Do not send—The JMB is not shared with JSS or a Service Now partner.
- Send all information except configuration—The JMB is shared with JSS or a Service Now partner without any device configuration information.
- Send all information with IP Addresses overwritten—The JMB is shared with IP addresses overwritten with asterisks (*).

The following is a sample of a JMB when the Send all information with IP Addresses overwritten filter is applied:

```
<root-authentication>
    </root-authentication>
    <name-server>
        <name>*.*.*.*</name>
    </name-server>
    <name-server>
        <name>*.*.*.*</name>
    </name-server>
    <name-server>
        <name>*.*.*.*</name>
    </name-server>
    <name-server>
        <name>*.*.*.*</name>
    </name-server>
    <radius-server>
        <name>*.*.*.*</name>
    </radius-server>
```

- **Send all information**—The JMB is shared as collected from a device.

The following is a sample of a JMB when the Send all information filter is applied:

```
<authentication-order>radius</authentication-order>
    <root-authentication>
```



```

</root-authentication>
<name-server>
  <name>192.0.2.4</name>
</name-server>
<name-server>
  <name>198.51.100.68</name>
</name-server>
<name-server>
  <name>203.0.113.101</name>
</name-server>
<name-server>
  <name>192.0.2.255</name>
</name-server>
<radius-server>
  <name>198.51.100.1</name>
</radius-server>

```

- Only send list of features used—The JMB is shared with the parameters configured without sharing the values configured for the parameters.

The following is a sample of a JMB when the Only send list of features used filter is applied:

```

<root-authentication>
  </root-authentication>
  <name-server>
    <name></name>
  </name-server>
  <name-server>
    <name></name>
  </name-server>
  <name-server>
    <name></name>
  </name-server>
  <name-server>
    <name></name>
  </name-server>
  <name-server>
    <name></name>
  </name-server>
  <radius-server>
    <name></name>
  </radius-server>

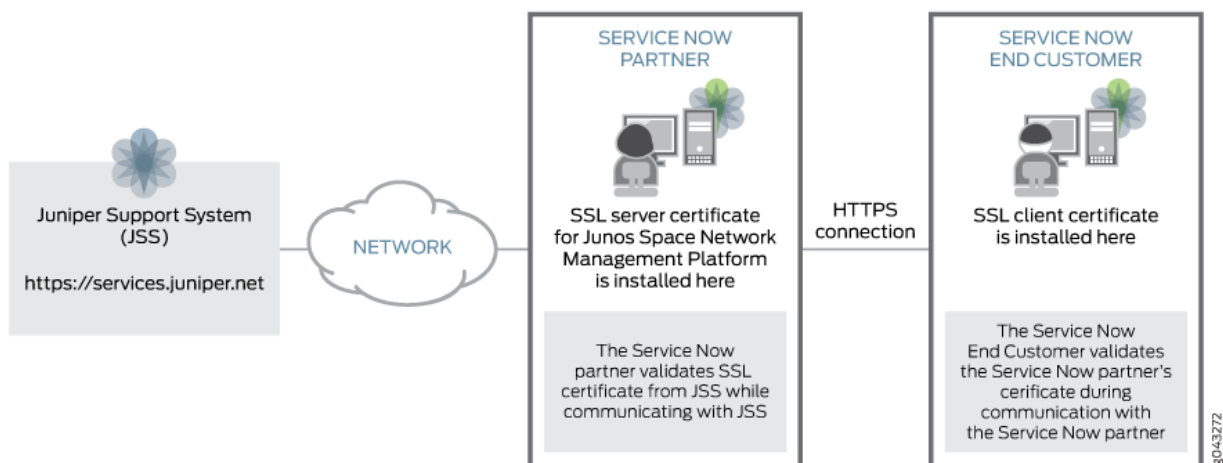
```

Service Now End Customer–Partner Communication Overview

A Service Now end customer establishes connection with a Service Now partner by using the HTTPS protocol. When a Service Now end customer initiates a request for communication with the Service Now partner, the Service Now partner provides a Secure Sockets Layer (SSL) certificate for the Service Now end customer to validate. The Communication between the Service Now partner and Service Now end customer is established after the Service Now end customer validates the certificate.

Figure 11 on page 78 depicts the communication between a Service Now partner with a Service Now End Customer and Juniper Support Systems (JSS) by using an SSL certificate.

Figure 11: Service Now Partner Communicating with a Service Now End Customer and JSS Using SSL Certificate



For information about using SSL certificates, see [Certificate Management Overview](#).

By default, Junos Space Service Now uses a self-signed SSL certificate, provided by the Junos Space Network Management Platform, to validate connections between a Service Now partner and Service Now end customers. However, from Service Now Release 14.1R3, a Service Now partner can use a custom SSL certificate instead of the default self-signed certificate to secure communication with Service Now end customers.

To secure the communication between a Service Now partner and Service Now end customer, perform the following tasks:

1. [Generating CSR by Service Now Partner](#) | 79
2. [Obtaining Signature of a Certificate Authority](#) | 82

3. [Uploading the Certificate to Service Now Partner | 82](#)
4. [Obtaining the Intermediate Certificate \(key\) for Establishing Credibility of the SSL Certificate | 82](#)
5. [Obtaining SSL Certificate of the Service Now Partner | 83](#)

Generating CSR by Service Now Partner

To install a custom SSL certificate on the Service Now partner, you must first generate a Certificate Signing Request (CSR):

To generate a CSR:

1. Log in to the Junos Space Appliance.

The Junos Space Settings Menu Is displayed.

2. Type **7** if the Junos Space Appliance is a virtual appliance or type **6** if the Junos Space Appliance is a hardware appliance to access the SSH shell.

3. Change the directory to **/etc/pki/tls**.

```
[root@host] cd /etc/pki/tls
```

4. Open the **openssl.cnf** file and comment out all instances of **subjectAltName=\${ENV::SAN}**.

```
<snip>
# subjectAltName=${ENV::SAN}
<snip>
```

5. Save the file.

6. Generate a private key by executing the following command:

```
server $ openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
```

Where 1024 is the length of the key in bits and `server.key` is the name of the key file.

7. Enter a pass phrase for the private key.

```
server $  Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

8. Generate a signing request using the private key and password.

You are prompted to provide your details such as the state or province to which you belong, your locality, email address and so on.

```
server $ openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:Sydney
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Juniper
Organizational Unit Name (eg, section) []:AS
Common Name (e.g. server FQDN or YOUR name) []:he-man
Email Address []:fred@juniper.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:fred1234
An optional company name []:
server $
```

After this step is executed, you can find the following encrypted files in the `/etc/pki/tls` folder:

- **server.key**—The private key for the SSL certificate.

The following is a sample of the **server.key** file obtained by using the `cat server.key` command:

```
server $ cat server.key
-----BEGIN RSA PRIVATE KEY-----
```

```

Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 019649A2E4BBCC4C

uKKzDLcMrBpuYDkxSl6epQqoScvcYnJvTM5kaJKNNxVrUarYA16JYFsZBOEpqCjr
AV7Ln6hg8Jl+UPEbrZPvXVED29qvM4tp1SDwKwuLs+IRWSON9ee2TsmVubCE0Ac7
aA8jg7kzubCktF3y+8/lM3yf+IWMY4EdWBXWtjMBO22kjU5KGWyznQeCsN2HtOLp
WvFOFDQHgxougL0qfF7pkDsVby5bKv74OT+ju/On6HtLf8IUfZDh/Xui/scsoKeb
8eJnNKNoldYAtU+eyNwkmPl09j8Ly/GeeiOOamMFaDpO1WuMQLmEH8En3tVIULrD
WZ2Ly0U9+d6Jl6f7LXXIEcBcH0eOOC3pp7Bq4zlk0/2WPq5FmcM9OmZZdeC2ZeYP
fNzBk2lZVVDAM89ggNlRNsm6FG9F6kkfczjBOSvawhBs7AgTDzty5J279uTGiyol
lCVXbi jo9+KR3INX3nWatYyR7T7MUGlYma/MbCg2dWAPR6iwYWy3w6VD51BIGNCP
po42YOH4yLvT8OuVzKpQ8z9tjukO5ZAR6E8fWEdiYBbPIhfEBxc7WVUBdPE/OQaj
8FuyLnzY5iCxYltkyWhtXntX32NrHJdJp6A8HfJf/v3ZnJ8FRHrNXtALcENVkgit
iCgmsGr5zwThiJqdSp6Xd4YpJrws5baTGRNjOrhfunGyEebhYmsQVKZpuXYM/YuV
5/Nqd3Hdmx58hWXViOCm7+HULRFRCu+JBhBLOJ9rBzaDVAFRqNtkMkFlwHKQ6u9K
ly+qgO7gT8jYIWgfKsB70QdMF+MntA+SvD5bfoUd6CY=
-----END RSA PRIVATE KEY-----

```

- **server.csr**—The CSR file to be signed by a Certificate Authority (CA).

The following is a sample of the **server.csr** file obtained by using the **cat server.csr** command:

```

server $ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwfTElMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UE
BxMGU3lkbmV5MRAwDgYDVQQKEwdkdW5pcGVyMQswCQYDVQQLEwJBuZEPMA0GA1UE
AxMGAguTbWFWuMR8wHQYJKoZIhvcNAQkBFhBmcmVhZGp1bmlwZXIubmV0MIGfMA0G
CSqGSIb3DQEBBQUAA4GNADCBiQKBgQCjA2megTM4/9iP9I56iNqmKmROQYfPwHLn
pW7BWq1Dikzn8BqM6cFeMalvUpRntiPJRNbUjGZPbf3cwZEy/vgy3MyTALFj9Zy
7tkpUIdlQn2KhW47mEcaixkEec5PxOUZm3Af1kKcMtIzajxxyVRs6cr6xLy0Bqew
1TA+3Xj6PwIDAQABOBkwFwYJKoZIhvcNAQkHMqoTCGZyZWQxMj0MA0GCSqGSIb3
DQEBBQUAA4GBAJjxApGFYAFfUllx0osdoGzedRkrVmR5693+hOEtI01n0z7ONCVu
ix0in4dH0SDipNPgfZwQ0jx6wyVGx/b6wWpMxBTrvhxH1EiCgR9pP0U63eMZsyEI
3RoU+7KeRTxxtXbRYUx0EHGPDHSGiShbjVc2uAPXijSRlutI3sViTJ2
-----END CERTIFICATE REQUEST-----

```

Obtaining Signature of a Certificate Authority

The Service Now partner should get the **server.csr** file signed by a Certificate Authority (CA); for example, GeoTrust[®], by contacting the CA. A signed certificate has the **.der** or **.pem** extension.

NOTE: Service Now supports signed certificates in the x.509 format only. We recommend that while requesting a CA to sign your certificate, specify that you need the signed certificate in the x.509 format.

After you receive the signed certificate, save it on your local system.

Uploading the Certificate to Service Now Partner

The signed **server.csr** file should be uploaded to the Junos Space Platform on which the Service Now partner is installed.

For information about uploading custom SSL certificate to Junos Space Platform, refer to [Installing Custom SSL Certificate on Junos Space Server](#).

Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate

Download the certificate key from the website of the CA from whom you obtained the signature for the SSL certificate; for example, <https://www.geotrust.com/resources/root-certificates/> is the website of GeoTrust[®].

Ensure that you select the appropriate root certificate and upload the root certificate obtained from the CA to the Junos Space Platform by using the **Administration > CA/CRL Certificates** navigation path of the Junos Space Platform GUI. For more information, see [Certificate Management Overview](#).

Obtaining SSL Certificate of the Service Now Partner

To secure communication with the Service Now partner, a Service Now end customer should obtain and install the SSL certificate from the Service Now partner.

NOTE: The procedure to obtain SSL certificate of a Web server varies from one browser to another.

To obtain the SSL certificate of the Service Now partner using Mozilla Firefox Web browser:

1. Open Mozilla Firefox Web browser and enter the URL to access the Service Now partner.

2. On the web browser, click the padlock present before the URL.

A dialog box with the information about the identity and security of the Service Now partner's Web site appears.

3. Click **More Information**.

The Page Info dialog box appears.

4. Click **Security > View Certificate** on the Page Info dialog box.

The Certificate Viewer dialog box appears displaying the SSL certificate used by the Service Now partner.

5. Click the **Details > Export** tab on the Certificate Viewer to export the SSL certificate.

The Save To dialog box of the web browser appears.

6. Save the certificate on your local system.

Ensure that the certificate is an X.509 certificate (*.pem).

To obtain the SSL certificate of the Service Now partner using CLI:

1. Connect to the Virtual IP (VIP) node of the Junos Space cluster on which the Service Now partner is installed and configured.

2. Type **7** if the Junos Space Appliance is a virtual appliance or type **6** if the Junos Space Appliance is a hardware appliance to access the SSH shell.

3. Type the following from the command line:

```
server $ echo "" | openssl s_client -connect <hostname>:443 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem
```

where *<hostname>* is the hostname of the Service Now partner.

SEE ALSO

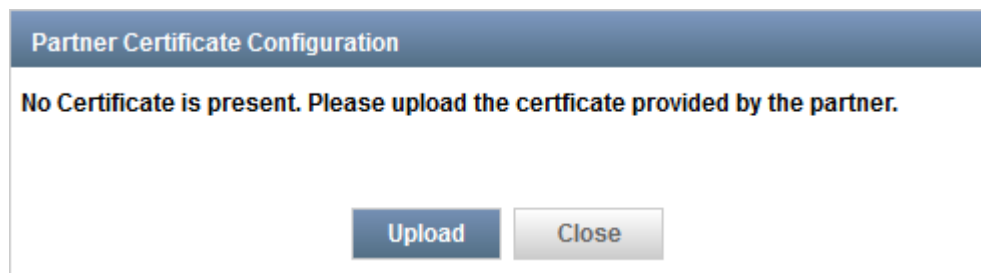
| [Installing the SSL Certificate on a Service Now End Customer](#) | 84

Installing the SSL Certificate on a Service Now End Customer

To install the SSL certificate obtained from Service Now partner on a Service Now end customer:

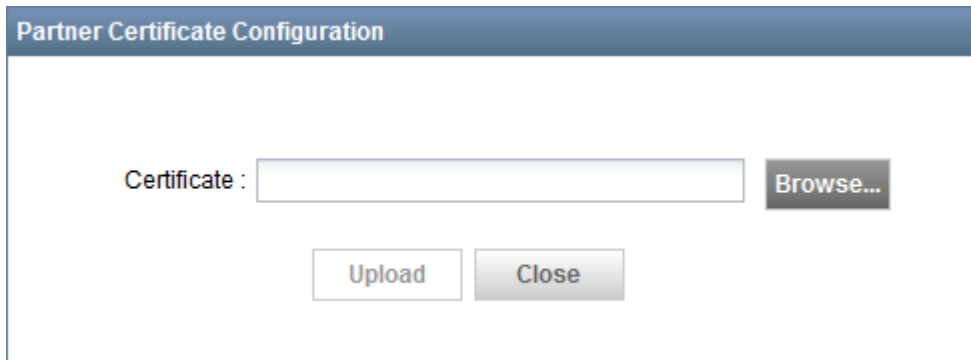
1. From the Service Now navigation tree, select **Administration** > **Global Settings** > **Partner Certificate Configuration**.

The Partner Certificate Configuration page appears. This page displays the certificates currently used by Service Now end customer. If the Service Now end customer does not have any certificate, this page displays the option to upload a certificate.



2. Click Browse to navigate and locate the certificate in your file system and then and then click **Upload**.

The Service Now GUI displays the option to browse and upload the certificate.



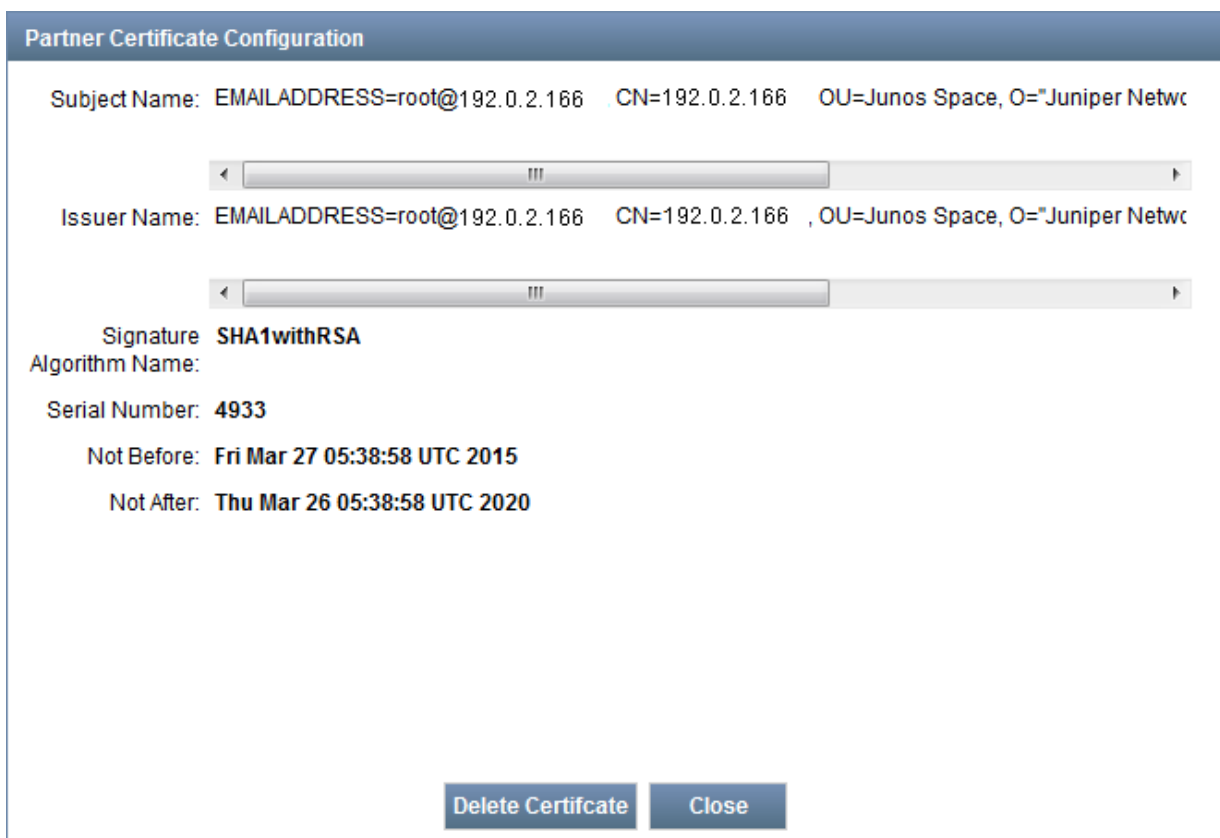
Partner Certificate Configuration

Certificate : **Browse...**

Upload **Close**

3. Click **Upload**.

The certificate is uploaded and displayed in the Partner Certificate Configuration page.



Partner Certificate Configuration

Subject Name: EMAILADDRESS=root@192.0.2.166 CN=192.0.2.166 OU=Junos Space, O="Juniper Netw

Issuer Name: EMAILADDRESS=root@192.0.2.166 CN=192.0.2.166 , OU=Junos Space, O="Juniper Netw

Signature **SHA1withRSA**

Algorithm Name:

Serial Number: **4933**

Not Before: **Fri Mar 27 05:38:58 UTC 2015**

Not After: **Thu Mar 26 05:38:58 UTC 2020**

Delete Certificate **Close**

RELATED DOCUMENTATION

5

CHAPTER

Deploying Service AI-Scripts, Service Now, and Service Insight Solution

Deploying AI-Scripts, Service Now, and Service Insight Overview | **89**

Installing and Configuring a Junos Space Appliance | **89**

Prerequisites for Deploying Junos Space Service Now and Service Insight | **90**

Determining Device Connections with Junos Space Nodes | **93**

Installing Junos Space Service Now and Junos Space Service Insight Applications | **94**

Discovering Devices | **98**

Configuring Service Now | **104**

Service Now and Service Insight Implementation Models | **127**

Deploying AI-Scripts, Service Now, and Service Insight Overview

Deploying AI-Scripts, Service Now, and Service Insight for Automated Support and Preventing (ASAP) solution involves the following tasks:

- Installing and configuring the Junos Space Network Management Platform (as a Juniper Networks JA2500 Junos Space Appliance or a Junos Space Virtual Appliance); see [“Installing and Configuring a Junos Space Appliance” on page 89](#) for details
- Installing Junos Space Service Now and Junos Space Service insight; see [“Installing Junos Space Service Now and Junos Space Service Insight Applications” on page 94](#) for details.
- Discovering Devices; see [“Discovering Devices” on page 98](#) for details.
- Adding devices to Service Now; see *Adding Devices to Junos Space Service Now* for details.
- Configuring Service Now; see [“Configuring Service Now” on page 104](#) for details.

Installing and Configuring a Junos Space Appliance

Junos Space Service Now and Junos Space Service Insight 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](#) | 94

[Configuring the Operating Mode of Junos Space Service Now](#) | 106

Prerequisites for Deploying Junos Space Service Now and Service Insight

IN THIS SECTION

- [Junos Space Platform Requirements](#) | 91
- [Device Requirements](#) | 91

For deploying the Service Now and Service Insight solution, the following Junos Space Platform and the managed devices should meet the following requirements:

Junos Space Platform Requirements

The requirements from Junos Space Platform are:

- A compatible version of the Junos Space Platform installed and fully configured.

NOTE: For information about Junos Space Platform releases compatible with a Service Now and Service Insight release, see [Junos Space Application Compatibility](#).

For information about installing and configuring the Junos Space Platform, see the *Juniper Networks JA2500 Junos Space Appliance* or the *Junos Space Virtual Appliance* guides at [Junos Space Network Management Platform Documentation Index](#).

- The following must be configured on a Junos Space Platform to implement the Service Automation solution:
 - IP addresses for eth0 and eth0:0 ports
 - (Optional) IP address for the eth3 port
 - (Optional) Network Address Translation (NAT) between the Junos Space appliance and JSS
If Junos Space-initiated connection is used, NAT can be implemented between the Junos Space Platform and device network.
 - A default gateway reachable by the Junos Space Platform
 - The firewall on Junos Space Platform is configured to connect with JSS (services.juniper.net) or Service Now partner to submit incidents. For information about ports used to connect to JSS or Service Now partner, see the *Firewall* section of the [“Junos Space Network Management Platform Hardening” on page 60](#) topic.

Device Requirements

The requirements from managed devices are:

- Devices should be running Junos OS release 11.4R1.0 or later.
- Devices must be installed with domestic Junos OS and configured for SSH and NETCONF.

```

system {
  services {
    netconf {
      ssh;
    }
  }
}

```

If devices are running worldwide (ww) Junos OS, the ww adapter must be installed on Junos Space.

- A user must be configured on the device with super user class for copying JMB files from `/var` to `/var/tmp`.

```

system {
  login {
    user lab {
      uid 2000;
      class super-user;
      authentication {
      }
    }
  }
}

```

- The following permissions must be set on the device for Junos Space Service Now to install AI-Scripts and collect JMBs:

```

set system login class servicenow permissions configure
set system login class servicenow permissions field
set system login class servicenow permissions maintenance
set system login class servicenow permissions network
set system login class servicenow permissions shell
set system login class servicenow permissions system
set system login class servicenow permissions view
set system login class servicenow allow-commands "((apply-groups juniper-ais)) ((request system software))|
((request system script)) ((stream)) ((text-pattern)) ((file copy)) ((ping)) | ((ftp))(((file)))"
set system login class servicenow allow-configuration "(system services)((system syslog)((system scripts))((groups
juniper-ais))((event-options)) (system commit synchronize))((ftp))((snmp))"
set system login class servicenow deny-configuration "((protocols))((routing-instances))((policy-options))((services))"
set system login user test class servicenow

```

RELATED DOCUMENTATION

Determining Device Connections with Junos Space Nodes

You can determine the devices connected to Junos Space from the devices or from Junos Space Network Management Platform.

To determine the connections between Junos Space Platform and managed devices, use the following commands:

- To determine the Junos Space instances to which a device is connected by device-initiated connection, issue the **show configuration system services outbound-ssh** command from the cli prompt of the device:

```
root@host> show configuration system services outbound-ssh
```

The following is a sample output of the command:

```
client 0050568a22c4 {
  device-id B9859F;
  secret "$ABC123; ## SECRET-DATA
  services netconf;
  192.0.2.100 port 7804;
}
client 000c297a03a8 {
  device-id 285AFF;
  secret "$DEF456"; ## SECRET-DATA
  services netconf;
  192.0.2.200 port 7804;
}
```

The output indicate that the device is connected to Junos Space nodes with IP addresses 192.0.2.100 and 192.0.2.200 through port 7804.

- To view active connections of the device with a Junos Space node, use **Show system connections** as follows:

```
root@host> show system connections | grep <ip address of Junos Space node>
```

The following is a sample output of the command:

```
root@host> show system connections | grep 192.0.2.51
tcp4          0          0  198.51.100.230.22          192.0.2.51.35181
ESTABLISHED
```

where 192.0.2.51 is the IP address of the Junos Space node and 198.51.100.230 is the IP address of the device.

- To get a list of all SSH connections on a Junos Space node, execute the **netstat -na** command from the shell prompt of a Junos Space node:

```
[root@host] netstat -na | grep 22
```

The following is a sample output of the command:

```
Output:-
tcp4          0          0  192.0.2.51.22
198.51.100.230.54732          ESTABLISHED
tcp4          0          0  192.0.2.51.22
198.51.100.235.33580          ESTABLISHED
```

where 198.51.100.230 is the device IP address and 192.0.2.51 is the IP address of the Junos Space node to which the device is connected.

RELATED DOCUMENTATION

Installing Junos Space Service Now and Junos Space Service Insight Applications

IN THIS SECTION

- [Uploading a Service Now and Service Insight Image File to a Junos Space Server | 95](#)
- [Installing Junos Space Service Now and Junos Space Service Insight | 97](#)

Junos Space Service Now Release 18.1R1 and Junos Space Service Insight Release 18.1R1 are supported only on Junos Space Network Management Platform Release 18.4R1. You must upgrade earlier releases of Service Now and Service Insight to 18.1R1 release for operating Service Now and Service Insight Release 18.1R1 on Junos Space Platform Release 18.4R1.



CAUTION: If Service Now and Service Insight are already installed on a Junos Space server, do not uninstall them to install or upgrade to a later version. Uninstalling deletes all the Service Now and Service Insight data from the Junos Space server. To upgrade Service Now and Service Insight to a later version, use the upgrade option in the Junos Space Network Management Platform. For details, see *Upgrading Junos Space Service Now and Junos Space Service Insight Applications*.

This topic discusses the following:

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.

NOTE:

- Service Insight is combined with Service Now in the Service Now image file. You can access Service Insight based on your license for support contract.
- You cannot access Service Insight if you are operating Service Now in the End Customer mode.

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 <https://www.juniper.net/support/downloads/?p=service-now#sw> 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 and select the Service Now image file 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 the 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 Junos Space Platform version is earlier than the compatible version, upgrade the Junos Space 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 *Upgrading Junos Space Network Management Platform Overview*.

- 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 95](#) for information about uploading an image file to 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 the Service Now Release that you want is listed, select it and click **Install**.

The Application Configuration window appears indicating that no configuration input is required..

- If the Service Now Release that you want is not listed, you must upload the release to Junos Space server.

To upload a 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 95](#).

5. Click OK.

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

6. 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.

7. After the installation job is complete, log out of Junos Space GUI and log in again 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

Junos Space Service Now Global Settings Overview

Configuring Global Settings

Discovering Devices

Before you add a device to Junos Space Service Now, Junos Space Network Management Platform should discover the device and upload the inventory and configuration of the device to the network management database.

Junos Space Platform discovers a device using SSH, SNMP, or ICMP ping. A device must fulfill the following prerequisites to be discovered by Junos Space Platform:

- The device should have the domestic Junos OS installed on it as domestic Junos OS contains the package for SSH support.

For devices running worldwide (ww) Junos OS, the devices must have the ww adaptor installed to allow Junos Space Platform to discover the device by using SSH.

- The device should have a management IP address configured on it and the management IP address should be reachable from the Junos Space server.
- The device should have a user with full administrative privileges configured on it..

- SNMP should be enabled on the device if you are using SNMP for discovering the device.
- Device should be configured to respond to ping requests if you are using ping for discovering the device.

For discovering a device, the Junos Space Platform always initiates the connection to the device and automatically enables SSH and NETCONF over SSH on the device by pushing the following commands:

```
set system services ssh protocol-version v2
set system services netconf ssh
```

To discover a device, the Junos Space Platform should have:

- A management IP configured and route enabled
- SSHv2 enabled
- NETCONF over SSH enabled
- If a firewall exists between the Junos Space Platform and device, the following ports must be opened:
 - TCP/22 to establish NETCONF over SSH connection with the device for device discovery
 - UDP/161 to perform SNMP queries on the device during device discovery
 - TCP/7804 to establish SSH connection to the Junos Space node if device-initiated connection model is used

NOTE: The following is a brief procedure for discovering a device. For the detailed procedure, see the *Discovering Devices* topic at [Junos Space Network Management Platform Documentation](#).

Discovering a device by the Junos Space Platform involves the following tasks:

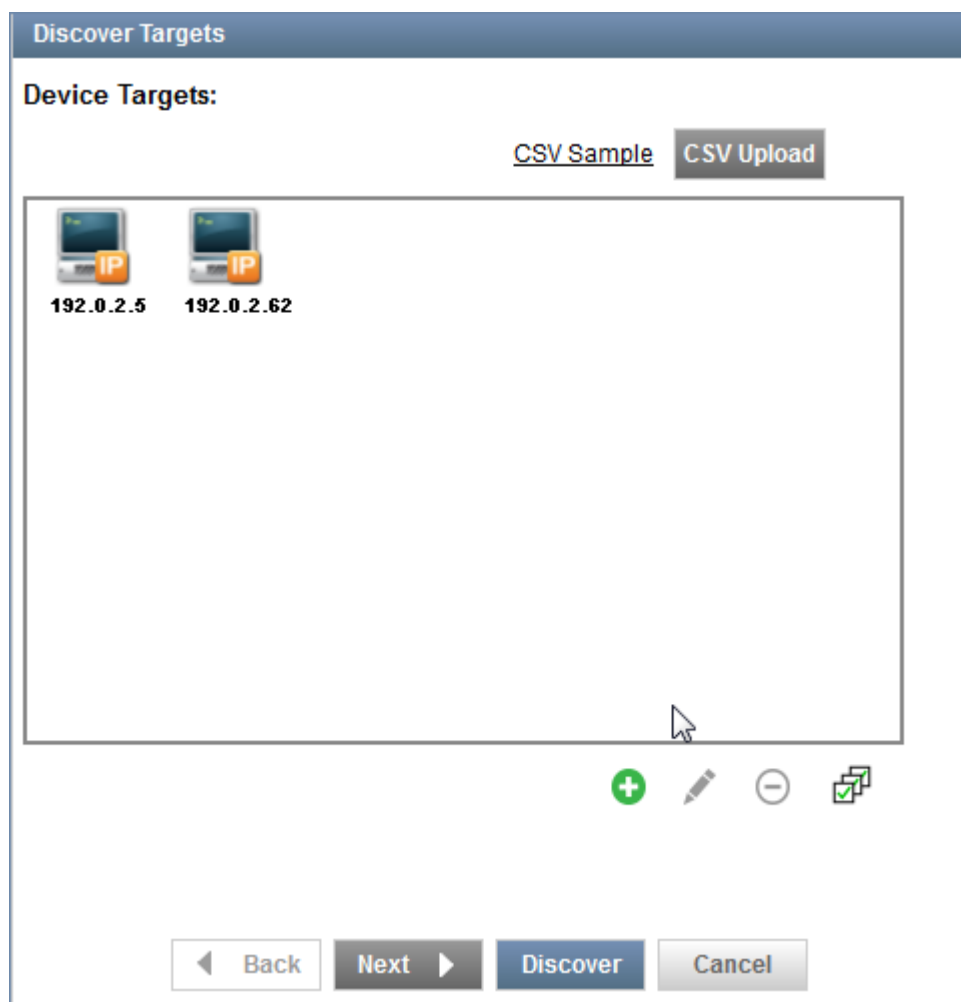
- a. Specifying device targets
- b. Specifying probes
- c. Specifying credentials

To discover devices in a managed network:

1. Log in to the Junos Space Platform GUI.
2. From the Network Management Platform navigation tree, select **Devices > Device Discovery > Discover Targets**.

The Discover Targets page appears as shown in [Figure 12 on page 100](#).

Figure 12: Device Targets Page



3. Click the **CSV Upload** button to add multiple device targets using a CSV file or the **Add** icon to add device targets manually.

Add devices by specifying any one of the following—IP address, IP address range, IP subnet, or hostname.

4. Click **Next** to specify probes to discover devices.

The Specify Probes page appears as shown in [Figure 13 on page 101](#).

Figure 13: Specify Probes Page

Specify Probes

☒ Use Ping

☒ Use SNMP

SNMP Settings:

- snmp v1/v2c public

+

✎

-

◀ Back Next ▶ Discover Cancel

5. Specify the method that the Junos Space Platform should use to discover devices.

- **SNMP:** Use this option if SNMP is configured on devices.
- **Ping:** Use this option if SNMP is not configured on devices.

This is the default option.

- **Use both SNMP and Ping to discover devices:** Use this option to use both SNMP and ping for discovering devices.

The discovery process is quicker when you use both SNMP and Ping.

If you are using SNMP, click **Add** to add SNMP settings; otherwise, go to the next step.

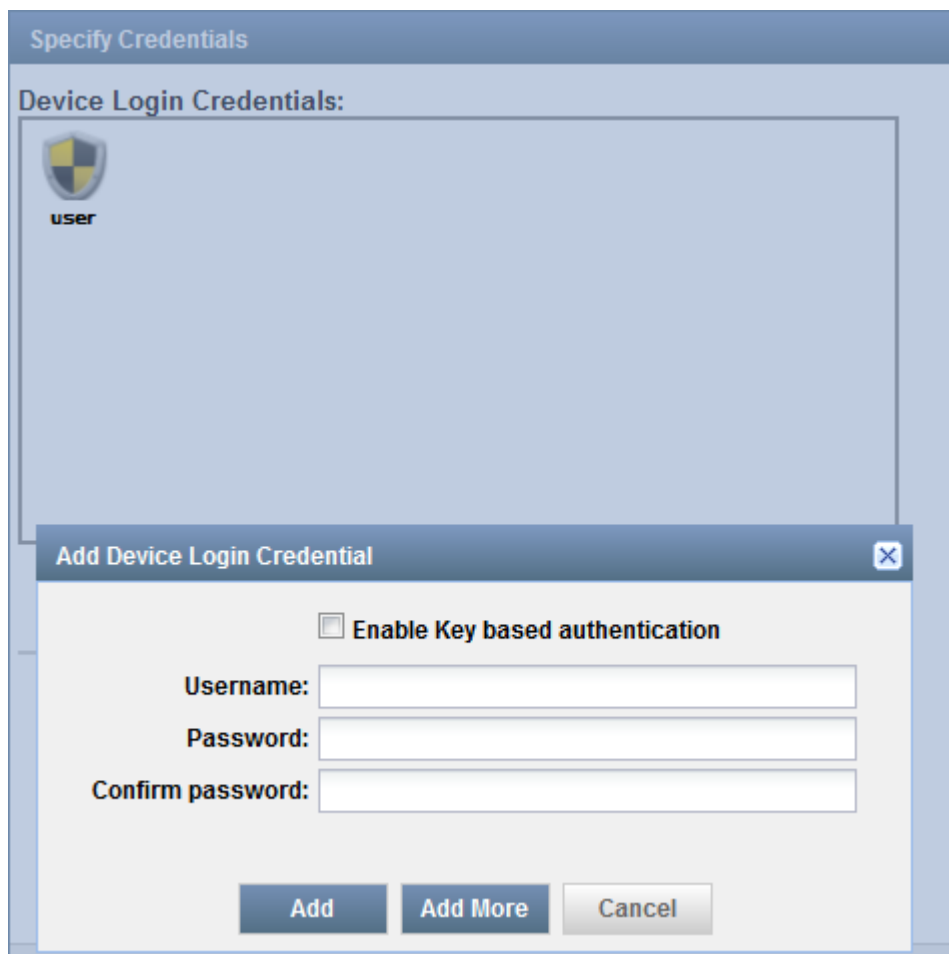
6. Click **Next**.

The Specify Credentials page is displayed.

7. Click the **Add** icon to add credentials to log in to devices in the managed network.

The Add Device Login Credentials dialog box is displayed [Figure 14 on page 102](#).

Figure 14: Add Device Login Credentials Dialog Box



The image shows a 'Specify Credentials' dialog box. Inside, there is a section titled 'Device Login Credentials:' which contains a shield icon and the text 'user'. Overlaid on this is a smaller 'Add Device Login Credential' dialog box. This sub-dialog has a checkbox labeled 'Enable Key based authentication'. Below it are three text input fields labeled 'Username:', 'Password:', and 'Confirm password:'. At the bottom of the sub-dialog are three buttons: 'Add', 'Add More', and 'Cancel'.

8. If you are using key-based authentication, select **Enable Key based authentication**.
9. In the **Username** and **Password** fields, enter the administrator username and password for a device in the managed network.

The name and password must match the name and password configured on the device. The username should be between two and 64 characters in length. The username should contain alphanumeric characters. Hyphen (-) and underscore (_) are allowed, but the username should not start with a hyphen. The user@domain.com format can also be used for the username.

There are no restrictions on the password.
10. (Optional) If you want to enter the administrator username and password for other devices in the managed network, click **Add More**.

11. Click **Add** to add usernames and passwords to the Device Login Credentials list.

12. Click **Discover** to discover devices.

The Discovery Status report appears. It shows the progress of device discovery in real time. Click a bar in the chart to view information about the devices currently being managed or discovered.

13. To view device discovery details, click **View Detailed Report**.

The report displays the IP address, hostname, and discovery status of the discovered devices.

If the discovery operation fails, the Description column in the Detailed Report table indicates the cause of failure.

You can view logs for the device discovery in the `/var/log/jboss/servers/server1/server.log` file. The following is a sample of the device discovery log for a device with IP address 10.207.72.117.

```
..eed to be set for ssh connection.
2015-04-23 13:26:55,932 WARN [net.juniper.jump.cmp.deviceManager.ejb.DeviceSvcAPI]
(EJB ts-pool - 2) Device Discovery Progress: ssh to device 192.0.2.117

2015-04-23 13:26:55,946 WARN [net.juniper.jump.cmp.deviceIOMgr.DmiDeviceSubjugator]
(Thread-83 (HornetQ-client-global-threads-1584673635)) Both username and password
need to be set for ssh connection.

2015-04-23 13:26:55,971 WARN [net.juniper.jump.cmp.deviceManager.ejb.DeviceSvcAPI]
(EJB ts-pool - 2) Device Discovery Progress: ssh to device 192.0.2.118

2015-04-23 13:26:55,984 WARN [net.juniper.jump.cmp.deviceIOMgr.DmiDeviceSubjugator]
(Thread-203 (HornetQ-client-global-threads-1584673635)) Both username and password
need to be set for ssh connection.

2015-04-23 13:26:56,000 WARN [net.juniper.jump.cmp.deviceManager.ejb.DeviceSvcAPI]
(EJB ts-pool - 2) Device Discovery Progress: ssh to device 192.0.2.119

2015-04-23 13:26:56,013 WARN [net.juniper.jump.cmp.deviceIOMgr.DmiDeviceSubjugator]
(Thread-164 (HornetQ-client-global-threads-1584673635)) Both username and password
need to be set for ssh connection.

2015-04-23 13:26:57,854 WARN
[net.juniper.jump.cmp.deviceIOMgr.DeviceInboundConnectionFactory] (Thread-83
(HornetQ-client-global-threads-1584673635)) Password authentication success for
192.0.2.117
```

Configuring Service Now

IN THIS SECTION

- [Configuring an SMTP Server | 104](#)
- [Configuring the Operating Mode of Junos Space Service Now | 106](#)
- [Configuring an Organization | 111](#)
- [Creating a Connected Member \(End Customer\) | 113](#)
- [Testing Service Now Connection | 114](#)
- [Creating Device Groups | 115](#)
- [Installing AI-Scripts on a Device | 117](#)
- [Creating Notification Policies | 123](#)
- [Generating Test Cases | 125](#)

Configuring Service Now involves the following tasks:

Configuring an SMTP Server

An SMTP server must be configured on the Junos Space Network Management Platform to submit incidents to Juniper Support Systems (JSS) or a Juniper Networks partner and receive responses for the incident.

To configure an SMTP server:

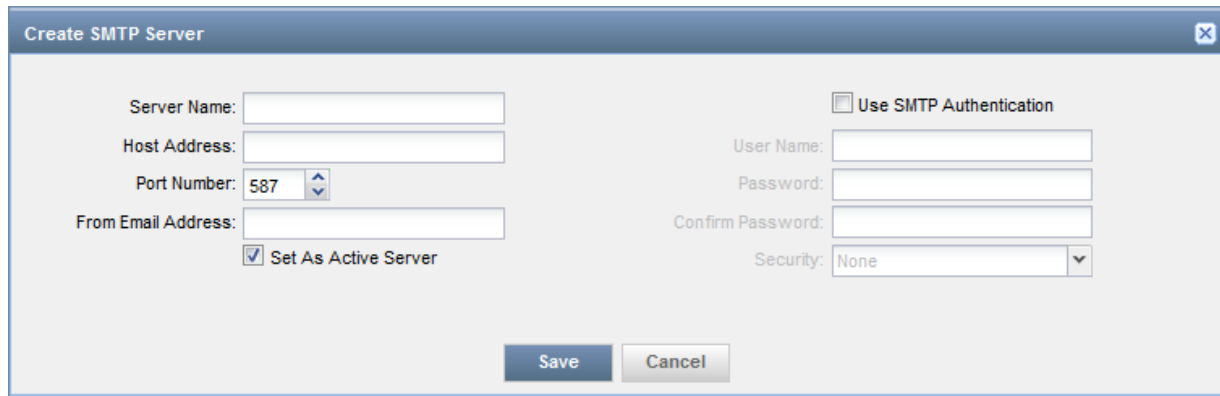
1. In the Network Management Platform navigation tree of the Junos Space GUI, select **Administration > SMTP Servers**.

The SMTP Servers page appears.

2. Click the **Add** icon.

The Create SMTP Server dialog box appears as shown in [Figure 15 on page 105](#).

Figure 15: Create SMTP Server Dialog Box



The dialog box titled "Create SMTP Server" contains the following fields and controls:

- Server Name:** A text input field.
- Host Address:** A text input field.
- Port Number:** A drop-down menu with "587" selected.
- From Email Address:** A text input field.
- Set As Active Server:** A checked checkbox.
- Use SMTP Authentication:** An unchecked checkbox.
- User Name:** A text input field (disabled).
- Password:** A text input field (disabled).
- Confirm Password:** A text input field (disabled).
- Security:** A drop-down menu with "None" selected.
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

3. In the **Server Name** field, enter a name for the SMTP server.

The name should contain alphanumeric characters and can include a hyphen (-), underscore (_), and period (.). The maximum number of characters allowed is 128.

4. In the **Host Address** field, enter the IP address of the mail server.

5. From the **Port Number** drop-down list, select a port number.

The default value is 587. This port number implies the use of SMTP server authentication.

6. In the **From Email Address** field, enter the e-mail address of this server in the format user@example.com.

This address appears as the sender of e-mail messages from the applications that are using this server.

7. (Optional) Select **Use SMTP Authentication** if you want the credentials of an e-mail to be checked before it is sent.

If you select Use SMTP Authentication, you must configure user credentials as follows:

- a. In the **User Name** field, enter a username for authentication.

There are no restrictions on the username.

- b. In the **Password** field, enter a password for the username.

There are no restrictions on the password.

- c. In the **Confirm Password** field, reenter the password for confirmation.

- d. From the **Security** drop-down list, select a protocol for encrypting e-mails sent through this server. The available options are Transport Layer Security (TLS) and Secure Sockets Layer (SSL).

For more information about configuring an SMTP server, see the *Junos Space Platform User Guide* at [Junos Space Network Management Platform Documentation](#).

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 16 on page 106 Global Settings page with options to configure the mode of operating Service Now.

Figure 16: Configuring Service Now Operating Mode

Global Settings ⓘ

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 mode by connecting 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” on page 23](#).

Ensure you have the following before configuring the operating mode of Service Now:

- If you want to configure offline mode on Service Now, you need a Partner Proxy or Direct mode license. You can obtain the license by contacting Juniper Networks Tech Support (JTAC) at [Juniper Networks support](#) and creating a technical service request.
- If you want to configure Partner Proxy or Direct mode on Service Now, you need to obtain the username and password for creating organizations. You can obtain the username and password for creating organizations by contacting Juniper Networks Tech Support (JTAC) at [Juniper Networks support](#) and creating a technical service request.
- If you want to configure End Customer mode on Service Now, you need to obtain the IP address of the Service Now partner and the username and password for creating an organization. You can obtain the IP address of the Service Now partner and the credentials for creating an organization by contacting the Service Now partner.

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 16 on page 106](#).

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 17 on page 108](#).

Figure 17: Offline Mode

Global Settings

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: ▼

☒ Collect Log Files

Note: Please enter the value as '0' in any of the fields above to set the purging interval to 'Never'.

☐ Direct Mode ☐ End Customer ☒ Offline Mode

Offline License:

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 Direct license and click **Upload**.
The license file is imported into Junos Space.
- c. Click **Save**.

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 18 on page 109](#) displays the Global Settings page for configuring Service Now in Direct mode.

Figure 18: Direct Mode

Global Settings ⓘ

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**

Note: Please enter the value as '0' in any of the fields above to set the purging interval to 'Never'.

☒ Direct Mode ☐ End Customer ☐ Offline Mode

To configure Service Now in the Direct mode, click **Save** 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*.

- End Customer mode

The Global Settings page for configuring Service Now in the End Customer mode is shown in [Figure 19 on page 110](#).

Figure 19: End Customer Mode

Global Settings

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**

Note: Please enter the value as '0' in any of the fields above to set the purging interval to 'Never'.

☒ End Customer

Enter IP or Hostname:

To configure Service Now to operate in End Customer mode:

- a. On the Global Settings page, click **End Customer**.

The Enter IP or Hostname text box appears.

- b. In the **Enter IP or Hostname** text box, enter the IP address or hostname of the Service Now partner and click **Save**.
- 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*.

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.

SEE ALSO

[Service Now Modes](#)

[Adding an Organization to Service Now](#)

[Testing Service Now Connection | 114](#)

[Adding an SNMP Configuration to Service Now](#)

Configuring an Organization

An organization represents the site ID of a customer in the Customer Relationship Manager (CRM) of JSS.

To create an organization, you need the site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks or a qualified Juniper Networks partner for operating Service Now in Direct or End Customer mode respectively. For operating Service Now in End Customer mode, the Service Now partner provides the username and password to configure an organization.

To configure an organization:

1. On the Junos Space Network Management Platform GUI, from the Service Now navigation tree, select **Administration > Organizations > Add Organization**.

The Add Organization page appears as shown in [Figure 20 on page 111](#).

Figure 20: Add Organization Dialog Box

2. In the **Name** field, enter a name for the organization.

The name should contain alphanumeric characters. Underscore(_), hyphen (-), and period (.) are allowed. The maximum number of characters allowed is 64.

3. From the **Submit Cases as** drop-down list, select Test Cases to submit incidents for testing purposes.

NOTE: You must change Test Cases to Real Cases after you complete testing. Otherwise, real-time incidents are submitted as test cases and will be ignored by JSS.

4. In the **User Name** and **User Password** fields, enter a username and password to log in to JSS to obtain a site ID.

5. Click the **Get Sites** button to obtain your site ID.

6. Select a filter level from the JMB Filter Level drop-down list.

The filter level determines what information in the JMB is shared with JSS or a Juniper Networks partner. The following filter levels are available:

- Do not send: Service Now does not send when you submit an incident.
- Send all information except configuration: Service Now sends JMBs without any device configuration information.
- Send all information with IP addresses overwritten: Service Now sends JMBs with IP addresses overwritten by asterisks (*). This is the default value.
- Send all information: Service Now sends the JMB as obtained from the device without any filtering.
- Only send list of features used: Service Now sends the JMB with the list of features (such as RADIUS server) configured on a device. However, the values configured for the features are not shared.

7. Click **Submit**.

The organization is created and listed on the Organizations page.

Creating a Connected Member (End Customer)

If you operate Service Now in the Partner Proxy mode, you must configure end customers (also known as connected members) to represent the Service Now end customer that connects with the Service Now partner.

To create a connected member:

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

The Add Member page appears as shown in [Figure 21 on page 113](#).

Figure 21: Add Member Dialog Box

Add Member

Name:

User Name:

User Password:

Confirm User Password:

JMB Filter Level:

Send all information with IP addresses overwritten

Select Configurations

<input type="checkbox"/> 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 end customer.

The name must contain only alphanumeric characters (a-z, A-Z, 0-9). The maximum number of characters allowed is 64.

3. In the **User Name** field, enter a username for the end customer.

The customer should use this username when submitting incidents for resolution to the Juniper Networks partner. The username must be in the user@example.com format.

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

There are no restrictions on the password.

5. In the **Confirm User Password** field, reenter the password.

6. From the **JMB Filter Level** drop-down list, select the JMB filter level.

The filter level determines the information in the JMB that can be shared with JSS.

7. Select **Override Address** if you want Return Materials Authorization (RMA) incidents from end customers to be submitted to JSS with your location or ship-to address.

If you do not select this check box, an RMA incident from an end customer is submitted to JSS with the end customer's location or ship-to address.

8. Select **Accept BIOS Validations** to accept BIOS data from end-customer devices 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 for the end customer.

9. Select **Accept AIS Health Check Incidents** to accept AI-Scripts health check incidents

10. Click **Submit**.

The end customer or connected member is created and listed on the Organizations page.

Testing Service Now Connection

After an organization is created, you can check whether or not you are able to connect to JSS or the Service Now partner (in case of End Customer mode).

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

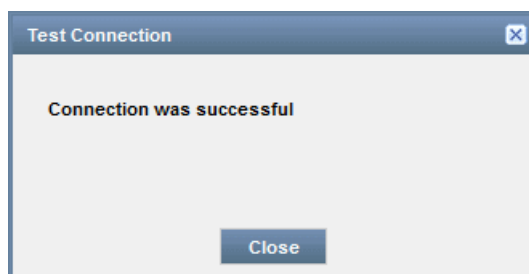
1. From the Service Now navigation tree, select **Administration > Organizations**.

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 22 on page 115](#).

Figure 22: 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.

SEE ALSO

Creating a Device Group

Service Now Device Groups Overview

Creating Device Groups

Devices that are discovered and added to the Junos Space Network Management Platform are automatically added to the Service Now application. However, if Junos Space Service Now is operating in demo mode, only the first five devices are added.

Device groups help manage devices as a single entity. You can group devices based on their functions or their attributes.

- If Junos Space Service Now is operating in the Direct mode, a default device group is automatically created and associated with an organization when you create the organization.
- If Service Now is operating in the Partner Proxy mode:
 - A default device group is automatically created and associated with an organization when you create the organization.

- A default device group is also added for the organization created by an end customer. Devices added to Service Now by the end customer are automatically added to the default device group. You can add or remove devices to or from the default device group in an end-customer organization, but cannot delete the default device group.

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 as shown in [Figure 23 on page 116](#).

Figure 23: Create Device Group Page

Create Device Group

Name:

Organization: [New Organization](#)

Select Devices to add them to the Device Group						
<input type="checkbox"/>	Host Name	Connected Member	Platform	IP Address	Serial Number	Version
No results to display						

Page 1 of 1

[Add](#) [Cancel](#)

2. In the **Name** field, enter a name for the device group.
The name must contain only alphanumeric characters (a–z, A–Z, 0–9). The maximum number of characters allowed is 64.
3. From the **Organizations** list, select an organization to which you want to add the device group.
If you want to add the device group to a new organization, click **New Organization**; see [“Configuring an Organization” on page 111](#) for details.

4. In the **Select Devices to add them to the Device Group** section, select the devices to be added to the device group.
5. Click **Add**.

The selected devices are added to the device group. To verify that the devices are added to the device group, double-click the device group on the Device Groups page to view the details of the device group.

Installing AI-Scripts on a Device

IN THIS SECTION

- Adding AI-Scripts Bundle to Service Now | 118
- Creating an Event Profile Using an AI-Scripts Bundle | 119
- installing the Event Profile on Devices | 121

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 generate 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.

NOTE: For information on resources utilized by AI-Scripts on a device, see [Effect of AI-Scripts on Resource Utilization of a Device](#).

Before you begin, ensure that you have the following:

- A valid service contract with Juniper Networks
- A 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

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.

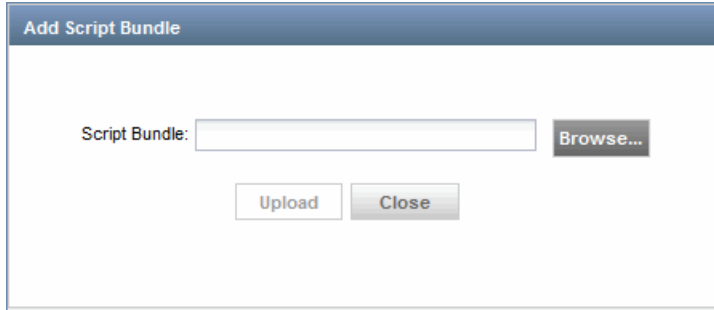
By default, the releases in the latest version are listed on the AI-Scripts - Download Software page.

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 24 on page 119](#).

Figure 24: 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 25 on page 120](#).

Figure 25: Add Event Profile Page

Add Event Profile

Profile Name:

Description:

Script Bundle: [Add Script Bundle](#)

Find Events: [Show Selected Events](#)

Event Synopsis	Type	Sub Type	Priority (editable)	KB Article	RMA Event
Category: ACCT (1 Item)					
<input checked="" type="checkbox"/> ACCT_XFER_POPEL_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_LZTP (1 Item)					

Page 1 of 5 | Displaying 1 - 100 of 435

[Submit](#) [Cancel](#)

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.

- 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:

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

The event profiles page appears.

- 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 26 on page 121](#).

Figure 26: Push to Devices Dialog Box

Push to Devices

Profile Name: Test_latest

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

Select Devices to Install Profile

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

Page 1 of 1

Displaying 1 - 9 of 9

☐ 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

Note:-

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

- 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 | 123](#)

[Generating Test Cases | 125](#)

[Manually Installing AI-Scripts on Devices](#)

[Juniper Networks Devices Supported by Service Now and Service Insight | 183](#)

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 27 on page 124](#),

Figure 27: Create Notifications Page

Create Notifications

Name:

Trigger:

Apply Filters

Priority:

Organization:

Device Group:

Device Name:

Serial Number:

Has the words:

Does not have:

Actions

Add Email Delete

☒ Email List

Send SNMP Traps to

Name
SNMP-Partner

Add Cancel

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.

SEE ALSO

Service Now Notification Policies Overview

[Generating Test Cases](#) | 125

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 28 on page 126).

Figure 28: 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.

SEE ALSO

Service Now Incidents Overview

Viewing Incident Details

RELATED DOCUMENTATION

Creating an Auto Submit Policy

Creating an Address Group

Configuring Product Health Data Collection on a Device

Configuring BIOS Validation for Verifying BIOS Integrity of a Device

Service Now and Service Insight Implementation Models

The ASAP solution uses both the Junos Space Service Now and Junos Space Service Insight applications. However, you can choose to use the capabilities of only Service Now or Service Insight as follows:

- To use the capabilities of Service Now only:
 1. Discover devices.
 2. Add the devices to a device group.
 3. Install AI-Scripts on the devices to detect events and collect intelligence information.

Based on the intelligence information collected from the device, Juniper Support Systems (JSS) continues to send end-of-life (EOL)/end-of-service (EOS) information and proactive bug notifications (PBNs) to Service Insight. The EOL/EOS information can be ignored if Service Insight is not used.

- To use the capabilities of Service Insight only:
 1. Discover devices.
 2. Add the devices to a device group.

NOTE: Do not install AI-Scripts on devices.

As AI-Scripts is not installed on devices, Service Now does not receive an intelligence Juniper Message Bundle (iJMB) within seven days from the device. As an iJMB is not received from the device, Service Now generates iJMBs using the **directive.rc** file. The process of using **directive.rc** file to generate a JMB is known as off-box method of generating a JMB. Service Now generates an iJMB using the **directive.rc** file when the device does not generate an iJMB between 7 and 12 days since Service Now received the last iJMB. The intervening days help in staggering off-box collection of iJMB to reduce network load and load on Junos Space Network Management Platform. Based on the iJMB generated by Service Now, JSS sends EOL/EOS and PBN notifications to Service Insight.

RELATED DOCUMENTATION

[Configuring Service Now | 104](#)

[Installing Junos Space Service Now and Junos Space Service Insight Applications | 94](#)

6

CHAPTER

Receiving Proactive Information from JSS

Proactive Information Received from Juniper Support Systems (JSS) | 131

Proactive Information Received from Juniper Support Systems (JSS)

IN THIS SECTION

- [PBN, EOL, and EOS Reports Overview | 131](#)
- [Generating a PBN Report | 131](#)
- [Generating an EOL Report | 135](#)

PBN, EOL, and EOS Reports Overview

The Service Insight application of the Automated Support And Prevention solution receives information about devices and device components nearing end-of-life (EOL) or end-of-service (EOS) and proactive bug notifications (PBNs) from Juniper Support Systems (JSS). PBNs help a network operator to identify devices that may be subject to potential bugs before the symptoms of the bugs are visible on the network.

The EOL information received includes end of engineering SW date, end of engineering HW date, end of sale parts, and end of support parts. PBNs usually indicate bugs related to disruption to traffic, sub-system outages in the control plane of a device, outages in a device or network due to input commands, and problems impacting business (for example, sampling of accounting parameters such as source class usage [SCU] and destination class usage [DCU]).

JSS generates EOL and EOS and PBN data by analyzing the informational JMBs (including off-box JMBs) received from the devices. Service Insight collects these notifications from JSS every midnight and displays them on the Exposure Analyzer page of the Service insight GUI.

A network operator can generate the EOL and PBN reports from the Exposure Analyzer page to identify devices nearing EOL or EOS and that are impacted by the received PBNs. For information about PBN and EOL reports, see [“Generating a PBN Report” on page 131](#) and [“Generating an EOL Report” on page 135](#).

Generating a PBN Report

A PBN report shows information about the number of devices that could be affected by potential bugs identified in the PBN notifications..

Figure 29 on page 132 shows a PBN report.

Figure 29: PBN Report

The screenshot shows a window titled "PBN Report Detail" with a close button in the top right corner. The window contains the following information:

- Name:** PBN4FromREST
- PBNs issued from:** Jan 29, 2015 9:19:45 AM IST
- PBNs issued till:** Apr 8, 2015 8:51:47 AM IST
- Date Created:** Apr 8, 2015 8:51:50 AM IST
- Last Ran On:** Apr 8, 2015 8:51:50 AM IST
- Created By:** user
- Devices Selected:** 3

Below this information are two scrollable lists:

- Device Name:** A list containing "Device1", "Device2", and "Device3".
- Recipients:** An empty list.

At the bottom left, it says "Devices Matching 1 PBNs:". At the bottom center is an "OK" button.

To generate a PBN report:

1. From the Service Insight navigation tree, select **Insight Central > Exposure Analyzer**.
The list of devices appears.
2. Select one or more devices for which you want to generate a PBN report.

- From the Actions menu, select **Generate PBN Reports**. Alternatively, right-click the device and select **Generate PBN Reports**.

The **Generate PBN Report** page appears as shown in [Figure 30 on page 133](#).

Figure 30: Generate PBN Report Page

Generate PBN Report

☐ Do not save this report on Service Insight

Enter PBN Report Name:

Create PBN Report for: ☐ All devices ☒ Selected devices shown below

Device Name	PBN Matches
Device1	Yes
Device2	Yes
Device3	Yes

Send Email To:

Add Email **Delete**

☐ **Email List**

☐ user@example.com

☐ Enter Email Id

PBN Issue date

Start Date and time: IST

End Date and time: IST

☐ ☒ **Schedule at a later time**

- (Optional) Select the **Do not save this report on Service Insight** check box if you do not want Service Insight to save the PBN report.

By default, Service Insight saves PBN reports..

5. Enter a name for the PBN report.

The name can contain alphanumeric characters (a–z, A–Z, 0–9), a space, an underscore (_), and a hyphen (-).

6. For the **Create PBN Report for** option, select one of the following:

- To generate PBN report for a particular organization or device group,

- a. Click **All devices**.

Organization and Device groups drop down menu are displayed.

- b. From the **Organization** or **Device Group** drop down menu, select the organization or device group for which you want to generate the EOL report.

- To generate PBN report for devices selected in step 2, click **Selected devices shown below**.

7. For the **Send Email To:** option, enter the e-mail address of the user to whom the PBN report must be sent.

To add and delete users who must receive the e-mail, use the **Add Email** and **Delete** buttons, respectively. By default, the **Send Email To** list contains the e-mail address of the logged-in user.

8. (Optional) Under the **PBN issue date** option, select values for **Start Date and time** and **End Date and time** to generate a report of the devices affected by PBNs issued during the selected time period.

NOTE:

- If a Start Date and time and End Date and time are not specified, managed devices in your network affected by all the PBNs issued by Juniper Support Systems (JSS) since the inception of JSS are reported.
- If you select only the start date and time, the devices in your network affected by all the PBNs issued from the selected Start Date and time till you generate the report are included in the report.
- If you select only the End Date and time, the devices in your network affected by all the PBNs issued by JSS since its inception and till the selected end date and time are included in the report.

9. (Optional) To schedule a time for generating the report, select the **Schedule at a later time** check box and set the date and time for the PBN report to be generated.

10. Select **Repeat** and schedule an interval for regenerating the PBN report.

The report generated for the first time has the name given by the user. For successive reports, the report name is appended with date and time the report is generated.

11. Click **Submit** after selecting the required options.

The Job Information dialog box displays a *job ID* link for the generated report.

If you have selected the **Do not save this report on Service Insight** check box, a **Download** link is provided to download the PBN report as an Excel file; otherwise, the PBN report is stored on Service Insight and can be viewed on the PBN Reports page (**Insight Central > PBN Reports**) after the job is completed.

12. (Optional) Click the *job ID* link.

The Jobs page displays the details of the generate PBN report job.

13. (Optional) If you want to cancel the scheduled job for generating the next PBN report, select the Create PBN Reports job and then select **Actions > Cancel Job**. Alternatively, right-click the job and select **Cancel Job**.

The job scheduled to generate PBN reports is cancelled.

Generating an EOL Report

An EOL report provides information such as the number of devices with EOL parts, EOL announce date, number of EOL announce parts, and Last Software Engineering Support date based on the EOL/EOS alerts received from JSS.

Figure 31 on page 136 shows an EOL report.

EOL Report Detail

Name: EOL1
Date Created: Apr 7, 2015 9:43:11 AM IST
Last Ran On: Apr 7, 2015 9:43:11 AM IST
Created By: super
Devices Selected: 8

Device Name
device1
device2
device3
...

Recipients
user@example.com

Status: Email successfully sent

Devices With EOL: 3
Parts:
End Of Life: 0
Announce Parts:
End of Sale Parts: 0
Last HW Engineering Parts: 2
Last SW Engineering Parts: 0
End of Service Parts: 2

OK

To generate an EOL report:

1. From the Service Insight navigation tree, select **Insight Central > Exposure Analyzer**.
The list of devices appears.
2. Select one or more devices for which you want to generate an EOL report.
3. From the Actions menu, select **Generate EOL Reports**. Alternatively, right-click the device and select **Generate EOL Reports**.

The **Generate EOL Report** page appears as shown in [Figure 32 on page 137](#).

Figure 32: Generate EOL Report Page

Generate EOL Report

☐ Do not save this report on Service Insight

Enter EOL Report Name:

Create EOL Report for: ☐ All devices
☒ Selected devices shown below

Device Name	EOL Data Available
srx-1400-sn1	Yes

Send Email To:

Add Email Delete

Email List
<input type="checkbox"/> user@example.com
<input type="checkbox"/> Enter Email Id

4. (Optional) Select the **Do not save this report on Service Insight** check box if you do not want Service Insight to save the EOL report.

By default, Service insight saves EOL reports.

5. In the **Enter EOL Report Name** field, enter a name for the EOL report.

The name can contain alphanumeric characters (a–z, A–Z, 0–9), a space, an underscore (_), and a hyphen (-).

6. For the **Create EOL Report for** option, select one of the following:

- To generate EOL report for a particular organization or device group,

- a. Click **All devices**.

Organization and Device groups drop down menu are displayed.

- b. From the **Organization** or **Device Group** drop down menu, select the organization or device group for which you want to generate the EOL report.
 - To generate EOL report for devices selected in step 2, click **Selected devices shown below**.
7. Enter the e-mail address of the users to whom the EOL report must be sent.
 To add and delete e-mail addresses, use the **Add Email** and **Delete** buttons respectively. By default, the **Send Email To** list contains the e-mail address of the logged-in user.
8. (Optional) To schedule a time for generating the report, select the **Schedule at a later time** check box and set the date and time for the EOL report to be generated.
9. (Optional) Select **Repeat** and schedule an interval for regenerating the EOL report.
 The report generated for the first time has the name given by the user. The successive reports are named by appending the name with the date and time, the report was generated.
10. Click **Submit**.
 The Job Information dialog box displays a *job ID* link for the generated report.
 If you have selected the **Do not save this report on Service Insight** check box, Service Insight displays a **Download** link to download the EOL report as an Excel file; otherwise, Service Insight stores the EOL report. You can view the EOL Reports page (Insight Central > EOL Reports) after the job is completed.
11. (Optional) Click the *job ID* link.
 The Jobs page displays the details of the generate EOL report job.
12. (Optional) If you want to cancel the scheduled job for generating the next EOL report, select the job and then select **Actions > Cancel Job**. Alternatively, right-click the job and select **Cancel Job**.
 The job scheduled to generate EOL reports are cancelled.

RELATED DOCUMENTATION

| [Exposure Analyzer Overview](#)

7

CHAPTER

Troubleshooting

Monitoring AI-Scripts Behavior by Using the AI-Scripts Event Simulator | **141**

Troubleshooting Failures While Discovering Devices | **143**

Troubleshooting AI-Scripts Installation Issues | **144**

Troubleshooting Issues with Generating JMBs | **149**

Troubleshooting Issues with Collecting JMBs | **150**

Troubleshooting Issues with Creating Incidents | **153**

Troubleshooting Issues with Submitting Incidents to JSS or a Service Now Partner | **154**

Troubleshooting Issues with Adding an Organization to Junos Space Service Now | **155**

Troubleshooting Issues with Receiving Notifications | **157**

Monitoring AI-Scripts Behavior by Using the AI-Scripts Event Simulator

With the AI-Scripts event simulator, you can generate error messages to monitor AI-Scripts behavior.

When the event simulator generates and enters an error message in the system logs of the device, the AI-Script pertaining to the event that caused the error message is triggered to generate a JMB for the event.

The event simulator is packaged with an AI-Scripts bundle starting from AI-Scripts Release 3.2R1.

To use the AI-Scripts event simulator for monitoring AI-Scripts behavior:

1. Log in to the device running Junos OS.
2. Verify that AI-Scripts Release 3.2R1 or later is installed on the device.

To verify that an AI-Scripts bundle is installed on the device, see [“Troubleshooting AI-Scripts Installation Issues” on page 144](#).

If not already installed, create an event profile by using AI-Scripts Release 3.2R1 or later and install the event profile on the device. To create and install an event profile, see *Adding an Event Profile to Junos Space Service Now* in the *Service Automation User Guide*.

3. On the device running Junos OS, run shell.
4. Navigate to the directory where the event simulator is located:

```
cd /var/db/scripts/op/.
```

5. Run the event simulator:

```
sh AIS_event_sim.sh
```

A menu of event types is displayed, as shown in the following sample:

```
AIS PROBLEM SIMULATION MENU (AI-Scripts 3.7R4/4.0R2 release)
=====

1. Hardware Failure
2. Software Failure
3. Resource Exhaustion Failure
4. Daemon crash [WARNING: This test could be service affecting as it kills the
daemon]
```

```

5. Unstructured Events
6. Events that may be triggered on a Backup Routing Engine (platform dependent)
7. Events added/modified to 3.3R1
8. Events added/modified to 3.3R2
9. Events added to 3.3R3
10. Events added/modified to 3.4R1
11. Events added to 3.5R1/3.4R2
12. Events added to 3.6R1
13. Events added/modified for 3.6R2/3.7R1
14. Events added/modified for 3.7R3/4.0R1
15. Events added/modified for 3.7R4/4.0R2
16. Exit

Please enter option [1 - 16]:

```

6. From the menu, select an event type and enter its number at the command prompt. For example, type **3** to generate error messages for a resource exhaustion failure event on the device.

A menu listing the events for the selected event type appears. The following menu appears when you type **3**.

```

RESOURCE EXHAUSTION FAILURE MENU
=====

1. ACCT_MALLOC_FAILURE
2. ASP_L2TP_NO_MEM
3. AUTOCONFD_AUTH_NO_MEM
4. CHASSISD_IPC_MSG_DROPPED
5. L2CPD_SCHED_SLIP
6. L2CPD_SYSTEM_CALL_FAILED
7. RPD_ISIS_OVERLOAD
8. RPD_OS_MEMHIGH
9. RT_SCREEN_TCP
10. RT_SCREEN_UDP
11. RTPERF_CPU_THRESHOLD_EXCEEDED
12. SNMPD_SUBAGENT_NO_RESOURCES
13. TASK_OS_MEMHIGH
14. VCCPD_PROTOCOL_OVERLOAD
15. Exit

Please enter option [1 - 15]:

```

7. Select an event from the menu and type its number at the command prompt.

The event simulator enters the error message in the system logs for the event that you select from this list.

8. Type the highest number on the menu to exit the program. For example, 15 in this case.

The CLI prompt appears.

9. Execute the following command to monitor the execution of the **cscript** process to verify that a JMB is created for the event.

show system processes extensive | match csc

10. Log in to the Junos Space GUI and navigate to **Service Now > Service Central > Incidents**.

An incident is generated in Service Now for the event that you generated using the event simulator. The incident is usually generated in Service Now within a few minutes after the event is generated on the device.

RELATED DOCUMENTATION

AI-Scripts Overview

Viewing Incident Details

[Troubleshooting AI-Scripts Installation Issues | 144](#)

Troubleshooting Failures While Discovering Devices

For information about troubleshooting failures while discovering devices, see [Troubleshooting Device Discovery Failure](#).

RELATED DOCUMENTATION

[Troubleshooting AI-Scripts Installation Issues | 144](#)

[Troubleshooting Issues with Creating Incidents | 153](#)

[Troubleshooting Issues with Receiving Notifications | 157](#)

Troubleshooting AI-Scripts Installation Issues

Problem

Description: The installation of AI-Scripts on a device running Junos OS fails.

Symptoms:

- The AI-Scripts bundle is not being installed properly on the device.
- During the installation of the event profile, the SLAX files are not copied to the device.
- AI-Scripts installed on a device do not generate a JMB for a particular event.

Resolution

Verifying the AI-Scripts Installation

To verify that an AI-Scripts bundle is installed on a device running Junos OS:

1. Log in to the device.
2. Run the **show version** command.

If the AI-Scripts bundle is installed on the device, the **show version** command lists the version of the AI-Scripts bundle installed on the device, as shown in the following sample:

```
Hostname: mx-80-sn2
Model: mx80-48t
JUNOS Base OS boot [11.4R6-S2]
JUNOS Base OS Software Suite [11.4R6-S2]
JUNOS Kernel Software Suite [11.4R6-S2]
JUNOS Crypto Software Suite [11.4R6-S2]
JUNOS Packet Forwarding Engine Support (MX80) [11.4R6-S2]
JUNOS Online Documentation [11.4R6-S2]
JUNOS Routing Software Suite [11.4R6-S2]
JUNOS AIS Script Suite [4.1R1.1]
```

The presence of **JUNOS AIS Script Suite** in the output of the **show version** command indicates that AI-Scripts Release 4.1R1.1 is installed on the device.

3. If you do not find **JUNOS AIS Script Suite** in the output of the **show version** command, see:

- *Installing an Event Profile on a Device by Using Service Now* to install AI-Scripts on devices managed by Service Now using the Junos Space GUI
- *Manually Installing AI-Scripts on Devices* to install and configure AI-Scripts on the devices manually

Resolving Issues with Copying Event Scripts to Devices

During the installation of an event profile on a device, the SLAX files are not copied to the devices and the Jobs status page displays an error as shown in [Figure 33 on page 145](#).

Figure 33: Service Now Event Profile Install/Uninstall Status

Service Now Event Profile Install/Uninstall Status				
NetworkName	Host Name	JobType	Status	Reason
▼ 192.0.2.194	J1-RE0	Install	Failed	<p>Error: Failed to upload Event Profile on to the Master RE.</p> <p>Write to destination file (/var/db/scripts/commit/jais-SN-activate-scripts.slax) failed: Permission denied</p>
Event Profile Install/Uninstall steps		Status		
Connect to device		Success		
Copy script bundle to device		Success		
Commit configuration		Success		
Install script bundle on device		Success		
Copy slax file to device		Failed		
Commit slax file on device		Not Started		

To copy event scripts to devices:

1. Log in to the device running Junos OS.
2. Execute the following command to check permissions for `/var/db/scripts/commit`, `/var/db/scripts/event`, and `/var/db/scripts/op` directories:

```
# run file list /var/db/scripts/
```

The permissions for the `/var/db/scripts/commit`, `/var/db/scripts/event`, and `/var/db/scripts/op` directories should be `drwxrws---`.

```
drwxrws---  2 root  wheel   1024 Jan 30 15:27 commit
drwxrws---  2 root  wheel  21504 Jan 30 15:27 event
drwxrws---  2 root  wheel   1024 Jan 30 15:26 op
```

3. If the permissions are not as shown in the preceding example, enter configuration mode and navigate to the `/var/db/scripts` directory.
4. As root at the shell level, execute `chmod 2770` to set the directory permissions as `drwxrws---` for the `/var/db/scripts/commit`, `/var/db/scripts/event`, and `/var/db/scripts/op` directories.
5. Retry installing the event scripts.

Verifying the Event Scripts Installed on the Device

To verify the event scripts installed on the device:

1. Log in to the device.
2. Execute the `show configuration groups juniper-ais | display commit-scripts`

```
show configuration groups juniper-ais | display commit-scripts
```

The following output is displayed:

```
system {
  scripts {
    op {
      file ais-pt_attachment.slax;
      file ais-rma_attachment.slax;
      file ais_change_perm.slax;
      file ais_core_perm.slax;
      file on-demand.slax;
      file remove-jais.slax;
      file jais-commit-optimize.slax;
      file ais_arc.slax;
      file ais-attach-file.slax;
```

```

        file stop-ais-now.slax;
        file ais_signalSN.slax;
        file ais_core_chm.slax;
        file ais_all_chm.slax;
        file att_signalSN.slax;
        file ais-rsi-chk.slax;
        file ais-rsi-delay.slax;
        file ais-rsi-holdoff.slax;
        file ais-param-set.slax;
        file ais-sleep.slax;
        file ais-error.slax;
        file ais-health-report.slax;
        max-datasize 256m;
    }
}
}
event-options {
    event-script {
        max-datasize 128m;
        file UI_CMDLINE_READ_LINE.slax;
        file UI_NETCONF_CMD.slax;
        file bios.slax;
        file bios-interval.slax;
        file ACCT_MALLOC_FAILURE.slax;
        file ACCT_XFER_POPEN_FAIL.slax;
        file ASP_PGCP_IPC_MSG_WRITE_FAILED.slax;
        file ASP_PGCP_IPC_PIPE_WRITE_FAILED.slax;
        file AUDITD_RADIUS_OPEN_FAILED.slax;
        file AUDITD_RADIUS_REQ_CREATE_FAILED.slax;
        file AUDITD_SOCKET_FAILURE.slax;
        file AUTHD_AUTH_CREATE_FAILED.slax;
        file AUTHD_SERVER_INIT_BIND_FAIL.slax;
        file AUTHD_SERVER_INIT_LISTEN_FAIL.slax;
        file AUTHD_SETSOCKOPT_FAILED.slax;
        file AUTHD_SOCKET_FAILED.slax;
        file AUTOCONFD_AUTH_NO_MEM.slax;
        file AUTOD_RECV_FAILURE.slax;
        file AUTOD_SEND_FAILURE.slax;
        file AUTOD_SOCKET_CREATE_FAILURE.slax;
        file AV_PATTERN_TOO_BIG.slax;
        file AV_PATTERN_WRITE_FS_FAILED.slax;
        file BFDD_READ_ERROR.slax;
        file BFDD_WRITE_ERROR.slax;
        file BOOTPD_HWDB_ERROR.slax;
    }
}

```

```

        file CFMD_RTsock_OPEN_FAILURE.slax;
        file CHASSISD_BUS_DEVICE_OPEN_FAILURE.slax;
        file CHASSISD_CFEB_POWER_FAILURE.slax;
        file CHASSISD_CLOCK_FAILURE.slax;
        file CHASSISD_CMB_READBACK_ERROR.slax;
    }
    destinations {
        juniper-aim {
            archive-sites {
                /var/tmp/;
            }
        }
    }
}

```

If event scripts are installed on the device, and the AI-Scripts version is Release 5.0R1 or earlier, the **show configuration groups juniper-ais** command lists the event scripts (.slax files) from the AI-Scripts bundle that are installed on the device under **event-options**. If event scripts are not listed under **event-options** in the output, then either the event scripts are not installed on the device or if they are installed, the **juniper-ais** group is not applied to the device configuration.

To verify that the **juniper-ais** group is applied to the device configuration, run the **show configuration apply-groups** command.

```
show configuration apply-groups
```

The following output is displayed for the command:

```

## Last commit: 2014-08-26 14:00:40 PDT by lab
apply-groups [ re0 ASIA-ROUTING-REGION juniper-ais ];

```

If the **juniper-ais** group is not listed in the output, issue the following command to apply the **juniper-ais** group:

```
set apply-groups juniper-ais
```

Verify that the **juniper-ais** group is applied to the device configuration by executing the **show configuration groups juniper-ais** command to list the event scripts installed on the device.

[AI-Scripts Overview](#)

[Service Now Event Profiles Overview](#)

[Uninstalling an Event Profile from a Device](#)

[Monitoring AI-Scripts Behavior by Using the AI-Scripts Event Simulator | 141](#)

Troubleshooting Issues with Generating JMBs

Problem

Description: No JMB is generated on a device running Junos OS.

Solution

AI-Scripts generate JMBs when an event occurs on the device on which they are installed and store the JMBs in the `/var/tmp` directory of the device. Service Now then copies the JMBs and the attachments from the device to `/var/cache/jboss/SN/Jmb/output` of the Junos Space Appliance. The JMBs and attachments are deleted from the device after they are copied to the Junos Space Appliance. From the Junos Space Appliance, the JMBs along with the attachments are uploaded to Juniper Support System (JSS) when the incident is submitted to JSS for creating a case.

To troubleshoot issues with JMB generation:

1. Log in to the device.
2. Enter CLI mode and execute the `show log default-log-messages | match AIS_DATA_AVAILABLE` command.

An output similar to the following is displayed if the JMBs are generated.

```
<13>1 2014-09-23T05:41:21.719Z sn-space-ex6200-sys cscript - - -
AIS_DATA_AVAILABLE: JMB generation initiated for eventID=998
<13>1 2014-09-23T05:42:36.945Z sn-space-ex6200-sys logger - - - transfer-file:
Transferred /tmp/evt_op_i4fS37
<13>1 2014-09-23T05:51:29.139Z sn-space-ex6200-sys cscript - - -
AIS_DATA_AVAILABLE: To be Transferred : JMB ready for upload
/var/tmp/sn-space-ex6200-sys_998_ais_intel_20140923_054236 size=34089
<13>1 2014-09-23T05:54:08.446Z sn-space-ex6200-sys cscript - - -
AIS_DATA_AVAILABLE: To be Transferred : All attachments ready for upload
<13>1 2014-09-23T05:58:23.445Z sn-space-ex6200-sys cscript - - -
AIS_DATA_AVAILABLE: JMB generation initiated for eventID=995
<13>1 2014-09-23T06:09:58.222Z sn-space-ex6200-sys cscript - - -
AIS_DATA_AVAILABLE: To be Transferred : JMB ready for upload
/var/tmp/sn-space-ex6200-sys_ais_health_123456 size=10015
```

```
<13>1 2014-09-23T06:10:48.379Z sn-space-ex6200-sys cscript - - -
AIS_DATA_AVAILABLE: To be Transferred : All attachments ready for upload
```

If you do not find the AIS_DATA_AVAILABLE messages in the output, see [“Troubleshooting AI-Scripts Installation Issues” on page 144](#) to check whether the AI-Scripts bundle is properly installed on the device.

For assistance with resolving this issue, contact JTAC at <https://www.juniper.net/support/requesting-support.html>.

RELATED DOCUMENTATION

AI-Scripts Overview

Service Now Incidents Overview

[Troubleshooting Issues with Collecting JMBs | 150](#)

[Troubleshooting AI-Scripts Installation Issues | 144](#)

Troubleshooting Issues with Collecting JMBs

Problem

Description: Junos Space Service Now fails to collect JMBs.

Symptoms: Service Now does not list any JMBs.

Cause

- Firewall rules on the device prevent Service Now from collecting JMBs.
- AI-Scripts do not function properly.

Resolution

Setting Firewall Rules on the Device

Service Now may not be able to collect JMBs from a device running Junos OS if the device does not allow traffic to the localhost address (127.0.0.1). Service Now uses the loopback interface on a device running Junos OS for collecting JMBs.

Set the following firewall rules on the device running Junos OS for Service Now to communicate by using the loopback address:

```
set firewall family inet filter scp-block term ais-scp from source-address
127.0.0.1/32
    set firewall family inet filter scp-block term ais-scp from
destination-address 127.0.0.1/32
    set firewall family inet filter scp-block term ais-scp from protocol tcp
    set firewall family inet filter scp-block term ais-scp from port 22
    set firewall family inet filter scp-block term ais-scp then accept
Router001# show firewall family inet filter scp-block term ais-scp
from {
source-address {
127.0.0.1/32;
}
destination-address {
127.0.0.1/32;
}
protocol tcp;
port 22;
}
then accept;
```

If you do not want to use the loopback address, modify the firewall family configuration to use the device's management IP address for collecting JMBs.

Resolving an AI-Scripts Error

Service Now might be unable to collect JMBs as a result of an AI-Scripts error. AI-Scripts errors are logged in the Junos OS system logs as **AIS_DATA_AVAILABLE: ERROR:** as follows:

```
AIS_DATA_AVAILABLE: ERROR: rsi_done-timeout
AIS_DATA_AVAILABLE: ERROR: waiting_on_slax-timeout
```

The error may be caused by an issue in the Junos OS software (for example, a CLI command does not return the expected output) or can be due to an internal AI-Scripts error.

To troubleshoot issues with JMB collection because of an AI-Scripts error:

1. Log in to the device.
2. Execute the following commands to obtain the relevant logs and files for troubleshooting:

```
show log messages | match cscript
show log escript.log
show configuration groups juniper-ais | display commit-scripts | no-more
show configuration system | display inheritance
show version
file list /var/db/scripts/op/ detail
file list /var/tmp/ detail
show system storage detail
show system processes extensive | match csc
start shell
ps ax | grep ais exit
```

3. After collecting the files, do the following:
 - Look for related events that occurred when or just before an AI-Scripts error message is generated in the system log output.
 - Look for SLAX errors logged during the execution of any of the event scripts in the **escript.log** file.
 - Examine the error messages in the error JMB files that may be created.
 - Save the collected files for further investigation.
 - For AI-Scripts versions earlier than AI-Scripts Release 4.0, execute the **request support information** command and store and note the size of the output created.
4. During a maintenance window, uninstall the AI-Scripts package from the device.

NOTE: You must uninstall AI-Scripts manually from the backup Routing Engines by using the **request system scripts delete *jais package name*** command, where *jais package name* is the name of the AI-Scripts package installed on the backup Routing Engine.

5. Manually install the AI-Scripts package by using the **request system scripts add /var/tmp/*jais package name*** CLI command, where *jais package name* is the name of the AI-Scripts installation package. Save the output printed on the monitor.
6. For AI-Scripts Release 4.1R1 and later, if Junos OS Release 14.1R1 or later is installed on the device, generate a health report JMB to obtain necessary information about the AI-Scripts error.

To generate the health report JMB, execute the following command on the device running Junos OS:

```
op ais-health-report job-ID job-id-number
```

where, *job-id-number* is the number that you assign to the job.

7. If you continue to receive error messages, open a case with your technical support representative to investigate the issue further. Provide the following information with the case:

- All Junos OS CLI command output mentioned in [Step 2](#)
- Any error JMB files that you received
- Output when you manually installed AI-Scripts
- Version of Junos Space and Service Now that you used

RELATED DOCUMENTATION

[AI-Scripts Overview](#)

[Service Now Incidents Overview](#)

[Troubleshooting AI-Scripts Installation Issues](#) | [144](#)

Troubleshooting Issues with Creating Incidents

Problem

Description: Junos Space Service Now does not create incidents.

Symptoms: Service Now does not list any incident.

Solution

When an event occurs on an AI-Scripts-enabled device running Junos OS, a script in the AI-Scripts bundle is executed to compile the event report in the form of a JMB. Service Now reads the JMB from the device and stores the JMB temporarily in the `/var/cache/jboss/SN/Jmb/output` directory on the Junos Space server. An incident is created on Service Now a minute after the JMB is copied to the Junos Space server.

If you do not find any incidents on Service Now, do the following:

1. Check whether the JMB is generated on the device. See [“Troubleshooting Issues with Generating JMBs” on page 149](#).

2. Check whether the JMB is collected by Service Now. See [“Troubleshooting Issues with Collecting JMBs” on page 150](#).
3. Check whether the JMB is listed on **Service Central > JMB Errors**. To resolve errors in JMB, contact JTAC at <https://www.juniper.net/support/requesting-support.html>.

RELATED DOCUMENTATION

Service Now Incidents Overview

AI-Scripts Overview

Troubleshooting Issues with Submitting Incidents to JSS or a Service Now Partner

Problem

Description: Junos Space Service Now does not submit incidents and JMBs to JSS or a Service Now partner.

Symptoms: The status of an incident is set to Submission failed on the Incidents page.

Solution

Service Now submits the incidents automatically to Juniper Support System (JSS) or a Service Now partner if configured to do so. If the submission of an incident fails, Service Now sets the status of the incident to Submission failed on the Incidents page.

To troubleshoot issues with submitting incidents to JSS or a Service Now partner:

1. Log in to Junos Space.
2. Select Service Now from the drop-down menu above the Junos Space Network Management Platform navigation tree.

The Service Now navigation tree appears.

3. From the Service Now navigation tree, select **Service Central > Incidents**.

The Incidents page appears.

4. Double-click the incident with the Submission failed status.

The Incident Details page appears. In the Status field of the Incident Details page, the reason for the failure to submit the incident to JSS or the Service Now partner is specified.

Look in the `/var/log/jboss/servers/server1/serviceNow.log` file with the search string “Case Submit failed for Incident” for more details.

See *Accessing Junos Space Service Now and Junos Space Service Insight Logs* for information about accessing Service Now logs.

A common reason for the Submission failed status of an incident is disrupted network connectivity with JSS. Check whether you are able to connect to JSS by pinging <https://services.juniper.net>.

For further assistance with resolving this issue, contact JTAC at <https://www.juniper.net/support/requesting-support.html>.

RELATED DOCUMENTATION

| *Service Now Incidents Overview*

Troubleshooting Issues with Adding an Organization to Junos Space Service Now

Problem

Description: An organization cannot be configured in Junos Space Service Now.

Solution

An organization in Service Now represents a unique site ID in Juniper Support System (JSS). Site IDs are used by JSS to identify customers when providing technical support. You can have multiple organizations defined in Service Now to manage multiple sites.

To communicate with JSS or a Service Now partner (when Service Now is operating in End-Customer mode), a Service Now organization requires a site ID, login name, and password. The login name must be a contact associated with the site ID. When an organization is added to Service Now, Junos Space must communicate with JSS to validate information about the organization. If Service Now cannot validate the organization information, the organization is created, but an error is reported on the GUI.

Each organization has a site ID, username, and password. You obtain the site ID, username, and password from Juniper Networks. If the site ID, username, and password are provided correctly, Service Now creates the organization and connects the organization with JSS or the Service Now partner. If the site ID, username, or password entered is incorrect, an error message such as **Connection Failed: Username or Password incorrect** is displayed indicating that the site ID, username, or password is incorrect. Retry adding the

organization by entering the correct site ID, username, or password. If you are still unable to configure an organization, contact Juniper Customer Care at <https://www.juniper.net/support/requesting-support.html>.

If you receive a **Connection Failed: Internal Error** message:

1. Log in to the Junos Space Appliance.

The Junos Space Settings Menu appears.

2. At the menu prompt, enter **6** if the Junos Space Appliance is a hardware (JA2500 appliance) or **7** if the Junos Space Appliance is a virtual appliance used to access shell.
3. Retype the Junos Space password.
4. Check the JSS connection status to **services.juniper.net**. As ping is disabled, you can try connecting to port 443 of **services.juniper.net** by using either of the following commands:

- `telnet services.juniper.net 443`

Or

```
curl -k https://services.juniper.net:443
```

If you are able to connect to **services.juniper.net** by using the telnet command, your Junos Space node is able to communicate with **services.juniper.net**. To break the connection established using the telnet command, press Ctrl followed by] on your keyboard.

If you are still unable to connect to **services.juniper.net**, it is possible that access to **services.juniper.net** is blocked on your network. Contact your network administrator to resolve the issue.

If you are unable to add an organization, there might be issues with your Juniper Networks account. Contact Juniper Technical Assistance Center (JTAC) at <https://www.juniper.net/support/requesting-support.html> for support.

RELATED DOCUMENTATION

Service Now Organizations Overview

Adding an Organization to Service Now

Troubleshooting Issues with Receiving Notifications

Problem

Description: Junos Space Service Now is not sending notifications.

Solution

Conditions such as a new incident created, incident submitted to JSS or a Service Now partner, or case ID assigned to an incident prompt Service Now to send e-mail notifications or SNMP traps.

If a user does not receive a notification from Service Now:

- Check whether a notification is configured for the trigger condition.

1. Log in to the Junos Space GUI.

2. Select Service Now from the drop-down menu above the Junos Space Network Management Platform navigation tree.

The Service Now navigation tree appears.

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

The Notifications page appears.

4. Check whether a notification is configured for the required condition.

If a notification is not configured for the required condition, configure a notification. For information about configuring notifications, see *Creating and Editing a Notification Policy* in the *Service Automation User Guide*.

5. Generate the condition for triggering the notification and check whether the notification is received by the user.

- Check whether the configured notification is enabled.

1. On the Notification page, right-click the disabled notification and select **Enable/Disable Notifications**.

The Change Reaction Policies Status dialog box is displayed.

2. Click **Change Status**.

The notification policy is enabled.

3. Create the condition for triggering the notification and check whether the notification is received by the user.

- Check whether an SMTP server is configured on Junos Space.

To check whether an SMTP server is configured on Junos Space, navigate to **Administration > SMTP Servers** in the Network Management Platform navigation tree. If no servers are listed on the SMTP Servers page, no SMTP server is configured.

Configure an SMTP server and create the conditions for triggering the notification and check whether the notification is received by the user. For information about configuring SMTP servers, see *Adding an SMTP Server* in the *Junos Space Network Management Platform User Guide* at [Junos Space Network Management Platform documentation](#).

- If an SMTP server is configured on Junos Space, check whether the SMTP server is operational by pinging the SMTP server.
 - If you are able to ping and see the IP address of the SMTP server, but do not receive any responses to the ping, it is possible that ping is blocked in your network. Contact your Network Administrator for releasing ping on your network.
 - If you are unable to ping the SMTP server and receive **unknown host <SMTP server hostname>** message, ensure that DNS is configured on Junos Space and that Junos Space is able to reach the configured DNS. For information about configuring or modifying the DNS on Junos Space, see *Changing Network and System Settings for a Junos Space Appliance* or *Changing the Network and System Settings of a Junos Space Virtual Appliance* at [Junos Space Network Management Platform Documentation Index](#).
 - If you are unable to ping the SMTP server, try connecting by using the SMTP server port:

```
telnet <IP address of SMTP server> <SMTP server port>
```

If you are able to connect to the SMTP server by using the telnet command, it indicates that your Junos Space node is able to communicate with the SMTP server. To break the connection established using the telnet command, press Ctrl followed by] on your keyboard.

- Look in the “Caught Exception in EmailMessageSender.sendEmail” entry in the Service Now log files for more information.

The Service Now log files are present at `/var/log/jboss/servers/server1/`.

If you are unable to resolve the issue and need assistance, contact Juniper Technical Assistance Center (JTAC) at <https://www.juniper.net/support/requesting-support.html>.

RELATED DOCUMENTATION

Service Insight Notifications Overview

[Adding an SMTP Server](#)

8

CHAPTER

System Log Messages

System Log Messages Used by Junos Space Network Management Platform and
Service Now | **161**

System Log Messages Used by Junos Space Network Management Platform and Service Now

A device running Junos OS, managed by Junos Space Network Management Platform, if configured to send system log messages, uses NETCONF over SSH to send log messages with specific text patterns to Junos Space Platform. The following configuration on the device specifies the text patterns based on which system log messages are filtered and sent to Junos Space Platform:

```
set system syslog file default-log-messages
any info;
match "(FRU Offline)|(FRU Online)|(FRU insertion)|(FRU power)|(FRU
removal)|(commit complete)|(copying configuration to juniper.save)|(license
add)|(license delete)|(link UP)|(package -X delete)|(package -X
update)|(plugged in)|(requested 'commit'
operation)|(unplugged)|Transferred|ifAdminStatus|transfer-file|transitioned|CFMD_COM_DEFECT|
LFMD_3AH | RPD_MPLS_PATH_BFD|(Master Unchanged, Members Changed)|(Master
Changed, Members Changed)|(Master Detected, Members Changed)|(vc add)|(vc
delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup
changed)|(interface vcp-)|(AIS_DATA_AVAILABLE)";
structured-data;
```

NOTE: The configuration might differ depending on Junos OS version running on the device and the device model.

Table 15 on page 161 lists examples of some of the system log messages that are used by Junos Space Platform and Service Now.

Table 15: System Log Messages Used by Junos Space Platform and Service Now

Match Pattern	Example System Log Message
FRU Online	gin-ttt-vpel chassisd[1581]: CHASSISD_SNMP_TRAP7: SNMP trap generated: Fru Online (jnxFruContentsIndex 7, jnxFruL1Index 1, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName FPC: MPCE Type 2 3D @ 0/*/*, jnxFruType 3, jnxFruSlot 0)

Table 15: System Log Messages Used by Junos Space Platform and Service Now (continued)

Match Pattern	Example System Log Message
FRU insertion	pe1 chassisd[1581]: CHASSISD_SNMP_TRAP7: SNMP trap generated: FRU insertion (jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName PIC: @ 0/0/*, jnxFruType 11, jnxFruSlot 0)
FRU power	e1 chassisd[1581]: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power off (jnxFruContentsIndex 8, jnxFruL1Index 12, jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName PIC: 10x 1GE(LAN) SFP @ 11/0/*, jnxFruType 11, jnxFruSlot 11, jnxFruOfflineReason 8, jnxFruLastPowerOff 961451815, jnxFruLastPowerOn 840678231)
FRU removal	pe1 chassisd[1581]: CHASSISD_SNMP_TRAP7: SNMP trap generated: FRU removal (jnxFruContentsIndex 8, jnxFruL1Index 12, jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName PIC: 10x 1GE(LAN) SFP @ 11/0/*, jnxFruType 11, jnxFruSlot 11)
commit complete	Device mgd 56190 UI_COMMIT_PROGRESS [device@host message="commit complete"] Commit operation in progress: commit complete
copying configuration to juniper.save	Device mgd 60751 UI_COMMIT_PROGRESS [device@host message="copying configuration to juniper.save"] Commit operation in progress: copying configuration to juniper.save
link UP	vllc-barryst craftd[1676]: Minor alarm cleared, xe-12/0/0: Link down =====> link up, no trap.
package -X delete	Device mgd 56190 - - /usr/libexec/ui/package -X delete jais
package -X update	Device file 61129 - - /usr/libexec/ui/package -X update /var/tmp/jais-4.1R4.1-signed.tgz
plugged in	gin-ttt-vpe1 fpc11 MIC(11/0)(0): SFP plugged in
requested 'commit' operation	Device mgd 56190 UI_COMMIT [device@host username="user" command="commit" message="none"] User 'user' requested 'commit' operation (comment: none)
unplugged	gin-ttt-vpe1 fpc11 MIC(11/0)(8): SFP unplugged

Table 15: System Log Messages Used by Junos Space Platform and Service Now (*continued*)

Match Pattern	Example System Log Message
Transferred	Device root - - - transfer-file: Transferred /tmp/evt_op_86Cbup 2015-06-26T08:34:08.890+10:00 Device cscript - - - JMB_AVAILABLE: Transferred JMB file with correct permission
ifAdminStatus	gin-ttt-vpe1 mib2d[2427]: SNMP_TRAP_LINK_DOWN: ifIndex 605, ifAdminStatus up(1), ifOperStatus down(2), ifName ge-0/1/9
transfer-file	Device root - - - transfer-file: Transferred /tmp/evt_op_86Cbup
transitioned	gin-ttt-vpe1 fpc11 CLKSUNC: Transitioned to centralized mode
AIS_DATA_AVAILABLE	router cscript: AIS_DATA_AVAILABLE: JMB generation initiated for eventID=447

9

CHAPTER

Number of Devices Managed by Service Now

Number of Devices Managed by Service Now | **167**

Number of Devices Managed by Service Now

The number of devices supported by Service Now depends on the Junos Space appliance used to create the Junos Space fabric as follows:

- An eight-node fabric (six Junos Space nodes and two fault monitoring and performance monitoring (FMPPM) nodes) comprising only JA2500 Junos Space appliances can manage up to 25,000 devices.
- A fabric comprising Junos Space virtual appliances with the same specifications as that of a JA2500 Junos Space appliance can manage the same number of devices as the JA2500 device.

For JA2500 Junos Space device specifications , see [Junos Space Datasheet](#).

10

CHAPTER

Suggested Test Plans

[Junos Space Service Now Test Plan | 171](#)

[Junos Space Service Now Test Plan | 174](#)

[Junos Space Service Insight Test Plan | 177](#)

Junos Space Service Now Test Plan

IN THIS SECTION

- [Add an Organization | 171](#)
- [Discover Devices | 171](#)
- [Add a Device Group | 172](#)
- [Add Discovered Devices to Device Group | 172](#)
- [Install an AI-Scripts Bundle on a Device | 172](#)
- [Configure Notifications | 172](#)
- [Generate a Test JMB | 172](#)
- [Verify Incident Creation in Service Now | 172](#)
- [Submit the Incident to JSS | 173](#)
- [Verify whether a Case is Opened for the Incident | 173](#)

Junos Space Service Now collects information about events that occur on devices and submits them to Juniper Support System (JSS) for resolution.

The following is a suggested plan for testing Service Now capabilities:

Add an Organization

To add an organization, see [“Configuring an Organization” on page 111](#).

If Service Now is operating in Partner Proxy mode, add an end customer; see [“Creating a Connected Member \(End Customer\)” on page 113](#) for details.

Discover Devices

To discover devices, see [“Discovering Devices” on page 98](#).

Add a Device Group

To add a device group, see [“Creating Device Groups” on page 115](#).

Add Discovered Devices to Device Group

To add discovered devices to the device group, see *Adding Devices to Junos Space Service Now*.

Install an AI-Scripts Bundle on a Device

To install an AI-Scripts bundle on a device, see [“Installing AI-Scripts on a Device” on page 117](#).

Configure Notifications

To configure notifications, see [“Creating Notification Policies” on page 123](#).

Generate a Test JMB

To generate a test JMB, see *Generating On-demand JMBs*.

Verify Incident Creation in Service Now

To verify incident creation in Service Now:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, select **Service Central > Incidents**.

If an incident is created successfully, the Incidents page should list the on-demand incident generated in [“Generate a Test JMB” on page 172](#).

Submit the Incident to JSS

To submit the incident to JSS:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, select **Service Central > Incidents**.

The Incidents page lists the on-demand incident generated in [“Generate a Test JMB” on page 172](#).

3. Select the incident.
4. From the **Actions** menu, select **Submit Case**.

The Submit Case Options page appears.

5. Enter values for the fields in the Submit Case Options page.
6. Click **Submit**.

If the case is submitted successfully, the status of the case is set to Submitted on the incidents page.

See [Submitting an Incident to Juniper Support System](#) for more details.

Verify whether a Case is Opened for the Incident

To verify whether a case is opened for the incident in JSS, see [Viewing a Case in the Case Manager](#).

RELATED DOCUMENTATION

[Junos Space Service Insight Test Plan](#) | 177

Junos Space Service Now Test Plan

IN THIS SECTION

- [Add an Organization | 174](#)
- [Discover Devices | 174](#)
- [Add a Device Group | 175](#)
- [Add Discovered Devices to Device Group | 175](#)
- [Install an AI-Scripts Bundle on a Device | 175](#)
- [Configure Notifications | 175](#)
- [Generate a Test JMB | 175](#)
- [Verify Incident Creation in Service Now | 175](#)
- [Submit the Incident to JSS | 176](#)
- [Verify whether a Case is Opened for the Incident | 176](#)

Junos Space Service Now collects information about events that occur on devices and submits them to Juniper Support System (JSS) for resolution.

The following is a suggested plan for testing Service Now capabilities:

Add an Organization

To add an organization, see [“Configuring an Organization” on page 111](#).

If Service Now is operating in Partner Proxy mode, add an end customer; see [“Creating a Connected Member \(End Customer\)” on page 113](#) for details.

Discover Devices

To discover devices, see [“Discovering Devices” on page 98](#).

Add a Device Group

To add a device group, see [“Creating Device Groups” on page 115](#).

Add Discovered Devices to Device Group

To add discovered devices to the device group, see *Adding Devices to Junos Space Service Now*.

Install an AI-Scripts Bundle on a Device

To install an AI-Scripts bundle on a device, see [“Installing AI-Scripts on a Device” on page 117](#).

Configure Notifications

To configure notifications, see [“Creating Notification Policies” on page 123](#).

Generate a Test JMB

To generate a test JMB, see *Generating On-demand JMBs*.

Verify Incident Creation in Service Now

To verify incident creation in Service Now:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, select **Service Central > Incidents**.

If an incident is created successfully, the Incidents page should list the on-demand incident generated in [“Generate a Test JMB” on page 172](#).

Submit the Incident to JSS

To submit the incident to JSS:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, select **Service Central > Incidents**.

The Incidents page lists the on-demand incident generated in [“Generate a Test JMB” on page 172](#).

3. Select the incident.
4. From the **Actions** menu, select **Submit Case**.

The Submit Case Options page appears.

5. Enter values for the fields in the Submit Case Options page.
6. Click **Submit**.

If the case is submitted successfully, the status of the case is set to Submitted on the incidents page.

See [Submitting an Incident to Juniper Support System](#) for more details.

Verify whether a Case is Opened for the Incident

To verify whether a case is opened for the incident in JSS, see [Viewing a Case in the Case Manager](#).

RELATED DOCUMENTATION

[Junos Space Service Insight Test Plan](#) | 177

Junos Space Service Insight Test Plan

IN THIS SECTION

- [Generate an On-demand Device Snapshot | 177](#)
- [Check Whether Device Snapshots are Received by Service Now | 178](#)
- [Check Whether Device Snapshots are Uploaded to JSS | 178](#)
- [Generate PBN Report | 178](#)
- [Generate EOL Report | 179](#)

Service Insight receives and displays End-of-Life (EOL) and End-of-Service (EOS) alerts and Proactive Bug Notifications (PBNs) sent by Juniper Support System (JSS). JSS sends these alerts to Service Insight on the basis of the device snapshots sent by managed devices. For information about device snapshots, see [Device Snapshots Overview](#).

The following is a suggested plan for testing Service insight capabilities:

Generate an On-demand Device Snapshot

A device snapshot is generated by AI-Scripts once in seven days. If no device snapshot is listed in Service Now under **Service Central > Information > Device Snapshot**, you can generate on-demand device snapshots.

To generate an on-demand device snapshot:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, select **Service Central > Administration > Service Now Devices**.
3. Select a device.
4. From the Actions menu, **Create On-demand Device Snapshot**.

The On-demand Device Snapshot dialog box is displayed. On the On-demand Device Snapshot dialog box, the **Upload iJMB** and **Verify CPU Usage** are selected by default.

5. Click **Submit**.

A job is created for generating the iJMB. If iJMB is generated successfully, it is listed under **Service Central > Information > Device Snapshots**.

Check Whether Device Snapshots are Received by Service Now

To verify whether device snapshots are received by Service Now:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.

If the device snapshot in [“Generate an On-demand Device Snapshot” on page 177](#) is generated successfully, the device snapshot should be listed on the Device Snapshots page.

Check Whether Device Snapshots are Uploaded to JSS

To verify that the device snapshot is uploaded to JSS:

1. If not already logged in, log in to Service Now.
2. On the Service Now navigation tree, navigate to **Service Central > Information > Device Snapshots**.

If the device snapshot in [“Generate an On-demand Device Snapshot” on page 177](#) is uploaded automatically, its status is set to Uploaded on the Device Snapshots page.

Generate PBN Report

To generate PBN report, see [“Generating a PBN Report” on page 131](#).

Generate EOL Report

To generate EOL report, see [“Generating an EOL Report” on page 135](#).

RELATED DOCUMENTATION

[Junos Space Service Now Test Plan](#) | 171

11

CHAPTER

Appendix

Juniper Networks Devices Supported by Service Now and Service Insight | **183**

Juniper Networks Devices Supported by Service Now and Service Insight

Table 16 on page 183 lists all the Juniper Networks product series and devices supported by Junos Space Service Now Release 18.1R1 and AI-Scripts Release 7.0R4. For information about devices supported by Junos Space Network Management Platform, see [Devices Supported by Junos Space Network Management Platform](#).

Table 16: Devices Supported by Junos Space Service Now

Product Series	Devices
ACX Series	ACX500
	ACX1000
	ACX1100
	ACX2000
	ACX2100
	ACX2200
	ACX4000
	ACX5000
	ACX5048
	ACX5096

Table 16: Devices Supported by Junos Space Service Now (*continued*)

Product Series	Devices
EX Series	EX2200
	EX2300
	EX3200
	EX3300
	EX3400
	EX4200
	EX4200-Copper
	EX4300
	EX4500
	EX4550
	EX4550-40G
	EX4600
	EX6200
	EX6210
	EX8208
	EX8216
	EX9200
	EX9204
	EX9208
	EX9214
	Junos Fusion Data Center
	Junos Fusion Enterprise

Table 16: Devices Supported by Junos Space Service Now (*continued*)

Product Series	Devices
EX Virtual Chassis	EX3300-VC EX4200-VC EX4300-VC EX4500-VC EX4550-VC EX9204-VC EX9208-VC MIXED-MODE-EX-VC EX-XRE
FireFly	vSRX Firefly
J Series	J2320 J2350 J4350 J6350
Junos Fusion	Junos Fusion Data Center Junos Fusion Edge Junos Fusion Enterprise
LN Series	LN1000 LN2600
M Series	M7i M10i M40e M120 M320

Table 16: Devices Supported by Junos Space Service Now (*continued*)

Product Series	Devices
MX Series	MX5
	MX10
	MX80
	MX104
	MX240
	MX480
	MX960
	MX2008
	MX2010
	MX2020
	MX10003
	MX10008
	MX10016
	Junos Fusion Data Center
MX Series Virtual Chassis	MX-VC
PTX Series	PTX1000
	PTX3000
	PTX5000
	PTX10008
	PTX10016

Table 16: Devices Supported by Junos Space Service Now (*continued*)

Product Series	Devices
QFX Series	QFX3000
	QFX3000-G
	QFX3000-M
	QFX3500
	QFX3600
	QFX5100
	QFX5100-96S
	QFX5110-32Q
	QFX5110-48S
	QFX5100-96S
	QFX5200
	QFX10002
	QFX10002-36Q
	QFX10002-36Q-DC
	QFX10002-72Q
	QFX10002-72Q-DC
	QFX10008
	QFX10016
	NOTE: QFX3000, QFX3000-G, and QFX3000-M are supported only in AI-Scripts 4.1 as part of QFabric.
QFX Series Virtual Chassis	QFX-VC

Table 16: Devices Supported by Junos Space Service Now (*continued*)

Product Series	Devices
SRX Series	SRX100
	SRX110H-VB
	SRX210
	SRX220
	SRX240
	SRX300
	SRX320
	SRX320-PoE
	SRX340
	SRX345
	SRX550
	SRX550-M
	SRX650
	SRX1400
	SRX1500
	SRX3400
	SRX3600
	SRX4100
	SRX4200
	SRX5400, SRX5600, SRX5800
Virtual SRX Series	Firefly Perimeter, vSRX NOTE: vSRX devices running Junos OS release earlier than Junos OS 15.1x are called Firefly Perimeter.

Table 16: Devices Supported by Junos Space Service Now (*continued*)

Product Series	Devices
T Series	T320
	T640
	T1600
	T4000
	TX Matrix
	TX Matrix Plus
	TXP-3D
Virtual MX Series	vMX
Virtual route reflector (VRR)	VRR

RELATED DOCUMENTATION

<i>Adding Devices to Junos Space Service Now</i>
Installing AI-Scripts on a Device 117