



Service Automation

User Guide

Release
13.3



Modified: 2016-06-24

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

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

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

Service Automation User Guide

Release 13.3

Copyright © 2016, Juniper Networks, Inc.

All rights reserved.

Revision History

March 2014— Service Automation User Guide, Release 13.3

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xv
	Junos Space Documentation and Release Notes	xv
	Documentation Conventions	xv
	Documentation Feedback	xvi
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvii
Chapter 1	Introduction to Service Automation	19
	Service Automation Overview	19
Part 1	AI-Scripts	
	AI-Scripts Overview	21
	Working Modes of AI-Scripts	21
	Events Detected by AI-Scripts	22
	JMB Contents	22
Chapter 2	Installing AI-Scripts	27
	Downloading AI-Scripts Install Packages and Release Notes	27
	AI-Scripts Install Package Versioning	28
	AI-Scripts Install Locations on Devices	29
	Automatically Installing AI-Scripts Bundles	29
	Manually Installing AI-Scripts on Devices	29
Part 2	Junos Space Service Now	
Chapter 3	Service Now Overview	33
	Service Now Overview	34
	Service Now Overview	34
	Service Now Domain	37
	Assigning a Service Now Object to Another Domain	39
	Upgrading Service Now	39
	Upgrading Service Now	39
	Service Now MIBs	42
	Service Now MIBs	42
	Service Now Modes	42
	Service Now Modes	42
	Overview	43

	Service Now Dashboard and Workspaces Overview	45
	Service Now Dashboard Overview	45
	Service Now Workspaces	45
	Dashboard Gadgets	46
	Service Now Inventory Pages	48
	Filtering Inventory Pages on Service Now and Service Insight	48
	User Roles	51
	Service Now User Roles	51
Chapter 4	Using the Service Now Getting Started Assistant	53
	Service Now Getting Started Assistant Usage Overview	53
	Service Now Getting Started Assistant Usage Overview	53
Chapter 5	Trouble Ticket APIs Supported by Service Now	55
	Trouble Ticket APIs Overview	55
	Profiles Used by Service Now	56
	Setting up Java Based Web Service Client	56
	Accessing a Web Service	62
	Trouble Ticket APIs Supported by Service Now	63
	Error Messages Displayed by OSS/J Client	64
	Trouble Ticket Attributes Supported by Service Now	66
	Trouble Ticket Events Supported by Service Now	68
Chapter 6	Administration	71
	Administration Overview	71
	Organizations	72
	Organizations Overview	73
	Adding an Organization	75
	Adding a Connected Member	77
	Modifying Organization Parameters	79
	Deleting an Organization	79
	Test the Connection to JSS	80
	Viewing Messages Assigned to a Connected Member	81
	Running an Organization in Test Mode	82
	Updating Core File Upload Configuration	82
	Device Groups	83
	Device Groups Overview	83
	Creating a Device Group	83
	Modifying Device Groups	85
	Deleting Device Groups	85
	Service Now Devices	86
	Service Now Devices Overview	86
	Adding Devices from the Platform	90
	Installing an Event Profile on Devices Using Service Now	91
	Uninstalling Event Profiles from Devices	94
	Exporting Device Data in CSV and Excel Format	94
	Exporting Inventory Information in CSV Format	95
	Viewing Exposure	96
	Generating On-Demand Incidents	96
	Collecting RSI and System Log Files	100

Requesting RMA Incidents	103
Deleting a Device	105
Associating Devices with a Device Group	105
Modifying Auto Submit Policy	106
Viewing Incidents	107
Verifying Connection between Devices and FTP Server	108
Event Profiles and AI-Scripts	108
Event Profiles Overview	109
Adding an Event Profile	110
Cloning an Event Profile	114
Deleting Event Profiles	116
Viewing an Event Profile	116
Pushing an Event Profile to Devices	117
Displaying Devices Associated with an Event Profile	119
Setting an Event Profile as Default	120
Exporting Events Data in Excel Format	120
Adding a Script Bundle to Service Now	121
Setting a Script Bundle as Default	122
Deleting a Script Bundle from Service Now	122
Global Settings	123
Configuring Global Settings	123
Adding an SNMP Server	129
Editing and Deleting an SNMP Server	131
Managing SNMP Traps	131
Configuring Proxy Server Settings	132
Uploading Core Files Generated for Events	133
Auto Submit Policy	134
Auto Submit Policy Overview	135
Creating an Auto Submit Policy	136
Modifying an Auto Submit Policy	139
Deleting Auto Submit Policies	140
Exporting an Incidents Report	140
Changing the Status of Auto Submit Policies	141
Changing the Status of Dampening	143
Address Group	144
Address Group Overview	144
Creating Address Group	145
Modifying Address Group	145
Deleting Address Group	146
Associating Devices with an Address Group From an Address Group ILP	146
Associating Devices with an Address Group From an Organization ILP	148
Associating Devices with an Address Group from a Device Group ILP	149
Associating Devices with an Address Group From a Service Now Devices ILP	150
E-mail Templates	151
E-mail Templates Overview	152
Viewing E-mail Templates	153
Modifying E-mail Templates	153

Chapter 7	Service Central	155
	Service Central Overview	155
	Incidents	157
	Incidents Overview	158
	Assigning an Incident Owner	160
	Flagging an Incident to a User	161
	Checking Incident Status Updates	162
	Exporting Incident Data	163
	Deleting an Incident	164
	Submitting an Incident to Juniper Support Systems	165
	Viewing Incident Details	169
	Viewing Knowledge Base Articles Associated with an Incident	171
	Viewing a Case in the Case Manager	171
	Updating an End-Customer Case	172
	Uploading Core Files for Incidents	174
	Information	174
	Messages Overview	175
	Assigning Ownership	175
	Flagging a Message to Users	176
	Deleting a Message	177
	Scanning a Message for Impact	177
	Assigning a Message to a Connected Member	178
	Device Snapshots Overview	180
	Exporting Device Data to HTML	181
	Deleting Device Snapshots	182
	Viewing Device Snapshot Details	182
	JMB Errors	184
	JMBs with Errors	184
	Downloading JMBs with Errors	184
	Deleting JMBs with Errors	185
	Notifications	186
	Notification Policies Overview	186
	Creating and Editing a Notification Policy	187
	Enabling or Disabling a Notification Policy	194
	Deleting a Notification Policy	194
Part 3	Junos Space Service Insight	
Chapter 8	Introduction to Service Insight	199
	Service Insight Overview	199
	Service Insight Overview	200
	Service Insight Dashboard Overview	202
	Dashboard Gadgets	202
	Service Insight Domain Overview	205
	Assigning a Service Insight Object to Another Domain	206

Chapter 9	Insight Central	207
	Insight Central Overview	207
	Insight Central Overview	207
	Insight Central Overview	207
	Exposure Analyzer	208
	Exposure Analyzer	208
	Exposure Analyzer Overview	208
	Generating EOL Reports	210
	Generating PBN Reports	211
	Showing Matching PBNs	213
	Managing EOL Reports	213
	Managing EOL Reports	213
	EOL Reports Overview	213
	Exporting EOL Reports	214
	Deleting EOL Reports	215
	Regenerating EOL Reports	215
	Managing PBN Reports	217
	PBN Reports Overview	217
	Exporting PBN Reports	218
	Deleting PBN Reports	218
	Regenerating PBN Reports	218
	Managing PBNs	220
	Managing PBNs	220
	Targeted PBNs Overview	220
	Scanning PBNs for Impact	221
	Flagging PBNs to Users	222
	Assigning PBN Ownership	223
	Deleting PBNs	223
	E-Mailing PBNs	224
	Managing Notifications	224
	Managing Notifications	224
	Notifications Overview	224
	Creating and Copying a Notification	225
	Editing the Filters and Actions of a Notification	228
	Enabling and Disabling Notifications	228
	Deleting Notifications	229
Chapter 10	JSS Messages Reference	231
	LIC-1001	231
	LIC-1098	231
	LIC-1099	231
	LIC-2000	232
	LIC-2099	232
	LIC-3000	232
	LIC-4000	232
	LIC-4001	233
	LIC-4002	233
	LIC-4003	233
	LIC-4004	233

LIC-4005	233
LIC-4006	234
LIC-4007	234
LIC-4008	234
LIC-4009	234
LIC-4010	234
LIC_4011	235
PVS-1000	235
PVS-1001	235
PVS-1002	235
PVS-1006	235
PVS-1007	236
PVS-1008	236
PVS-1009	236
PVS-1010	236
PVS-1011	236
PVS-1100	237
PVS-1200	237
PVS-1201	237
PVS-1202	237
PVS-1203	237
PVS-1204	238
PVS-1205	238
PVS-1207	238
PVS-1210	238
PVS-1213	238
PVS-1214	238
PVS-1215	239
PVS-1216	239
PVS-1223	239
PVS-1226	239
PVS-1227	239
PVS_1230	240
PVS-1231	240
PVS-1232	240
PVS-8000	240
PVS-8001	240
PVS-8002	241
PVS-8006	241
PVS-9000	241
PVS-9999	241
SEC-1000	241
SEV-0001	241
SEV-0002	242
SEV-0003	242
VLD-1000	242
VLD-2000	242

Part 3

Index

Index	245
-------------	-----

List of Figures

Part 1	AI-Scripts	
	Figure 1: Attachment Section in JMB Generated by AI-Scripts 4.0 Release	25
Part 2	Junos Space Service Now	
Chapter 3	Service Now Overview	33
	Figure 2: Platform with Most Incidents Gadget	47
	Figure 3: Devices with Most Incidents Gadget	48
Chapter 6	Administration	71
	Figure 4: Manage Organizations Page	73
	Figure 5: Add Organization Dialog Box	75
	Figure 6: Add Member Dialog Box	78
	Figure 7: Test Connection Dialog Box	80
	Figure 8: Messages Assigned to Connected Member Page	81
	Figure 9: Create Device Group Page	84
	Figure 10: Select Devices to Add to Service Now and Click Submit Page	90
	Figure 11: Install Event Profile Dialog Box	92
	Figure 12: Potential Exposure to Known Issues Page	93
	Figure 13: On-demand Incident Dialog Box	98
	Figure 14: Create On-demand Incident Status Dialog Box	99
	Figure 15: Configure File Collections Dialog Box	101
	Figure 16: Request RMA page	104
	Figure 17: Modify Auto Submit Policy Page	107
	Figure 18: View Event Profiles Page	110
	Figure 19: Add Event Profile Page	111
	Figure 20: Potential Exposure to Known Issues Page	113
	Figure 21: Push to Devices Dialog Box	117
	Figure 22: Potential Exposure to Known Issues Page	118
	Figure 23: View Event Profiles Page	120
	Figure 24: Add Script Bundle Dialog Box	121
	Figure 25: Global Settings Page	127
	Figure 26: SNMP Trap Attribute Page	132
	Figure 27: Proxy Server Configuration Dialog Box	133
	Figure 28: Auto Submit Policy Page	135
	Figure 29: Auto Submit Policy Creation Page	136
	Figure 30: Choose Events to Include in Auto Submit Policy Page	137
	Figure 31: Change Auto Submit Policy Status Page	142
	Figure 32: Change Auto Submit Policy Dampening Status Page	143
	Figure 33: Associate Address Group to Devices Page	147
	Figure 34: Associate Devices to Address Group Page	149

	Figure 35: Associate Devices to Address Group Page	150
	Figure 36: E-mail Templates Page	152
Chapter 7	Service Central	155
	Figure 37: Service Central Gadgets	156
	Figure 38: Export JMB to HTML Dialog Box	163
	Figure 39: Submit Case Options Page	166
	Figure 40: Incident Detail Page	170
	Figure 41: End-Customer Cases Dialog Box	173
	Figure 42: Choose Connected Members Dialog Box	179
	Figure 43: Juniper Message Bundle	183
	Figure 44: View JMB Dialog Box	183
	Figure 45: Download JMB Errors Dialog Box	185
	Figure 46: Create Notifications Page	188
Part 3	Junos Space Service Insight	
Chapter 9	Insight Central	207
	Figure 47: Insight Central Landing Page	208
	Figure 48: Exposure Analyzer Page	209
	Figure 49: EOL Reports Page View	213
	Figure 50: Regenerate EOL Report Dialog Box	216
	Figure 51: PBN Reports page	217
	Figure 52: Regenerate PBN Report Dialog Box	219

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xv
Part 1	AI-Scripts	
	Table 2: Elements in the Manifest Section of a JMB	22
Part 2	Junos Space Service Now	
Chapter 3	Service Now Overview	33
	Table 3: Service Now Objects and Their Default Domains	38
	Table 4: Tasks Enabled for Service Now Modes	44
	Table 5: Service Now Workspaces	46
	Table 6: Filter-enabled Tables and Columns	49
	Table 7: Predefined Service Now User Roles and Permissions	51
Chapter 5	Trouble Ticket APIs Supported by Service Now	55
	Table 8: Trouble Ticket APIs Supported by Service Now	63
	Table 9: OSS/J Client Error Scenarios	64
	Table 10: Supported Trouble Ticket Attributes	67
Chapter 6	Administration	71
	Table 11: Organization Column Descriptions	73
	Table 12: Organization Credentials Page Field Descriptions	76
	Table 13: Add Event Profile Page Field Descriptions	111
	Table 14: XML File Information	124
	Table 15: Global Settings Command Buttons	126
	Table 16: Global Settings Parameters	128
	Table 17: Icons That Represent the Event Types and Their Descriptions	137
	Table 18: Auto Submit Policy Icons	142
Chapter 7	Service Central	155
	Table 19: Notification Policies Table Column Descriptions	186
	Table 20: Create Notification Policy Page Field Descriptions	189
Part 3	Junos Space Service Insight	
Chapter 8	Introduction to Service Insight	199
	Table 21: Service Insight Workspaces	202
	Table 22: Service Insight Objects and Their Default Domains	205
Chapter 9	Insight Central	207
	Table 23: Exposure Analyzer Page Icon Descriptions	209

Table 24: Device Details from the Exposure Analyzer Page	210
Table 25: EOL Reports Page and EOL Report Detail Dialog Box Fields Description	214
Table 26: PBN Reports Page and PBN Report Detail Dialog Box Fields Description	217
Table 27: Manage PBNs Page Fields Description	221
Table 28: Manage Notifications Page Fields Description	225
Table 29: Manage Notifications Page Field Description	226

About the Documentation

- [Junos Space Documentation and Release Notes on page xv](#)
- [Documentation Conventions on page xv](#)
- [Documentation Feedback on page xvi](#)
- [Requesting Technical Support on page xvi](#)

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.


If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

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

Documentation Conventions

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

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.

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Introduction to Service Automation

- [Service Automation Overview on page 19](#)

Service Automation Overview

Juniper Networks Service Automation is an end-to-end solution designed to streamline operations and enable proactive network management for Junos OS devices. This solution leverages the Junos OS embedded technology to maximize uptime and minimize downtime while streamlining operations and reducing operational expenses.

The solution consists of Advanced Insight Scripts (AI-Scripts), Junos Space Service Now and Service Insight applications, and Juniper Support Systems (JSS). AI-Scripts are installed on devices running Junos OS. Junos Space Service Now and Service Insight applications form the user interface, and JSS allows for delivery of relevant knowledge and insight to enable a transformed support experience.

All Juniper Networks customers can take advantage of the Service Automation capabilities as a deliverable of the Juniper Care and Juniper Care Plus programs. Juniper Networks partners can take advantage of the Service Automation capabilities through the Operate Specialist program. For more details, see <http://www.juniper.net/us/en/products-services/technical-services/>.

Service Automation is comprised of the following three components:

- **Advanced Insight-scripts (AI-Scripts):** AI-Scripts is the collection component of Service Automation and is installed on devices running Junos OS. Each AI-Script in the AI-Scripts bundle corresponds to a predefined event such as hardware failure, memory leakage, output voltage overload and is executed when the predefined event occurs on a device. When executed, AI-Scripts collect data about an event and the device configuration, bundle the data in a structured format called Juniper Message Bundle (JMB) and store the JMB at a defined location on the device. Service Now accesses the JMB from the device for analysis and resolution. AI-Scripts work in two modes—reactive and proactive.

In the reactive mode, the AI-Scripts collect data in response to a predefined event.

In the proactive mode, the AI-Scripts collect data on vital system functions of a device at predefined intervals.

- **Service Now and Service Insight:** Service Now and Service Insight are the management components of Service Automation.

Service Now accesses JMB generated in a device in response to an event, creates an incident for the event in the Service Now database and notifies the network operator about the event. The Network Operator can configure Service Now to automatically to submit the incident with the JMB to Juniper Support System (JSS).

Service Insight receives alerts called Proactive Bug Notifications (PBNs) from JSS and notifies the network operator about impending problems in the network. JSS also provides alerts for devices and services nearing end of life (EOL) to Service Insight.

- JSS: JSS is the analysis component of Service Automation. It comprises of knowledge repositories such as JSS Database, EOL/EOS database, and the Juniper CRM.

For customers with Juniper Care Plus Service contract, JSS sends alerts for devices and services nearing End of Life agreements. While resolving an issue received from a customer, JSS analyzes the nature of the issue and sends PBNs to warn other customers about similar issues that can impact devices in their network.

**Related
Documentation**

- [AI-Scripts Overview on page 21](#)
- [Service Now Overview on page 33](#)
- [Service Insight Overview on page 200](#)

PART 1

AI-Scripts

- [AI-Scripts Overview on page 21](#)
- [Installing AI-Scripts on page 27](#)

AI-Scripts Overview

Advanced Insight Scripts (AI-Scripts) provide the intelligence that devices need to automatically detect and report hardware and software failure or other functional abnormalities to ensure maximum network uptime. AI-Scripts are imported into Service Now in the form of script bundles. For information about adding script bundles to Service Now, see [“Adding a Script Bundle to Service Now” on page 121](#).

When AI-Scripts are installed on a device, the device is said to be AI-Scripts-enabled. An AI-Scripts-enabled device can automatically detect any defined event, such as failure to allocate memory for a process or failure of a hardware when it occurs, and report the event to the network operator. When an event occurs, AI-Scripts generate the data about the event and package the data in a structured format called a Juniper Message Bundle (JMB) and store it at a defined location on the device from where Service Now accesses it for resolution.

This section contains the following topics:

- [Working Modes of AI-Scripts on page 21](#)
- [Events Detected by AI-Scripts on page 22](#)
- [JMB Contents on page 22](#)

Working Modes of AI-Scripts

AI-Scripts work in the following modes to generate a JMB:

- **Reactive mode:** In reactive mode, the AI-Scripts collect data from a device when a predefined event, such as failure to allocate memory for a process or failure of a hardware, occurs on the device and store the data at a predefined location on the device from where Service Now accesses it for analysis and resolution. The JMB generated in this mode is known as an event JMB or eJMB.
- **Proactive mode:** In proactive mode, the AI-Scripts periodically collect data on vital system functions and store them at a predefined location on the device. This data is accessed by Service Now to monitor the device and to predict and prevent risks related

to the device. The JMB generated in this mode is known as an informational JMB or iJMB.

Apart from incident and informational JMBs, AI-Scripts also generate JMBs in response to an event triggered by a user. These JMBs are known as on-demand incident JMBs. When you submit an on-demand incident on a device by using Service Now, Service Now generates an on-demand incident JMB by executing preconfigured CLIs on the device.

Events Detected by AI-Scripts

AI-Scripts detect the following types of events:

- Common software events, including daemon and Packet Forwarding Engine crashes
- Common hardware events, such as PIC alarms
- Hardware platform-specific events, such ASIC issues

JMB Contents

A JMB has the following structure:

- Manifest: The JMB manifest contains a summary of the information primarily needed for creating and submitting a case with JSS for an event. [Table 2 on page 22](#) lists the elements present in a JMB manifest.

Table 2: Elements in the Manifest Section of a JMB

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> <pre><router-name><chassis-serial-number><YYYYMMDD-HHMMSS><sequence></pre> <p>where:</p> <p><i>router-name</i> specifies the hostname of the router</p> <p><i>chassis-serial-number</i> specifies the serial number of the router chassis</p> <p><i>YYYYMMDD-HHMMSS</i> specifies the date and time of the event on the device.</p> <p><i>sequence</i> varies from 001–999 and indicates the sequence of events when multiple events occur at the same time.</p> <p>A <i>sequence</i> number is present only if multiple events occur on 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 Clarify.</p>

Table 2: 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. The 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 RMA event on the device.
Event Type Group	<p>Classifies the events that occur on the device under the following categories:</p> <ul style="list-style-type: none"> • Hardware Failure • Software Failure • Resource Exhaustion
Event Type	<p>Specifies the type of event that occurred on the device. For example: MAC error, Process error.</p>
Problem Synopsis	<p>Specifies a summary of the event. This field is used to populate the Problem Synopsis field in Clarify.</p> <p>This field can be appended while submitting the incident for resolution.</p>
Problem Description	<p>Specifies a description of the event. This field is used to populate the Problem Description field in the Customer Relationship Management (CRM) system.</p> <p>This field can be appended while submitting the incident for resolution.</p>
Problem Priority	<p>Specifies the user'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>The possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low
Product Name	<p>Specifies the name of the product. This field is used to populate the Platform field in Clarify.</p>
Host Name	<p>Specifies the hostname of the router</p>

Table 2: Elements in the Manifest Section of a JMB (*continued*)

Element	Description
Version Information	Provides software version information in one of the following formats: <ul style="list-style-type: none"> • Maintenance release format • Beta release format • Service release format
Time of Event	Specifies the time at which the event occurred
Core Manifest	Specifies the core files generated for the event
Show Chassis Hardware	Specifies the results of the show chassis hardware command

- Trend data: The trend data provide information about the hardware and software operating parameters such as CPU and memory utilization of the Routing Engine and traffic statistics of the Packet Forwarding Engine of a device.

Trend data are provided for the following:

- Routing Engine
- Flexible PIC Concentrators
- Packet Forwarding Engine
- Switch Control Board (SCB)
- Routing protocol process (RPD)
- Kernel
- Attachment: The files and data in a JMB depend on the type of the event that triggered the JMB. This section provides the output of specific Junos OS commands executed to retrieve data and log files pertaining to the event. Some commands are standard—that is, they are executed for every platform. Some commands are executed specific to a platform. The following commands are common to all platforms:
 - **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**

The JMBs generated by AI-Scripts Release 3.7 and earlier contain outputs of all executed Junos OS commands in a single file. The JMBs generated by AI-Scripts Release 4.0 contain links that you can click to view or download the output of the executed Junos OS commands as shown in [Figure 1 on page 25](#).

Figure 1: Attachment Section in JMB Generated by AI-Scripts 4.0 Release

Juniper Message Bundle(JMB)					
Manifest					
Trend data	Attachments details				Click here to download all attachments
Attachments	Command	File type	Size (Bytes)	View	Download
Logs	JMB event attachments	text	4843	View	Download
	show configuration display inheritance display xml except password except secret except -key except ssh-rsa except community-name	xml	4843	View	Download
	show chassis hardware detail display xml	xml	3393	View	Download
	show version display xml	xml	1184	View	Download
	request support information	text	4843	View	Download

Related Documentation

- [Adding a Script Bundle to Service Now on page 121](#)
- [Deleting a Script Bundle from Service Now on page 122](#)

CHAPTER 2

Installing AI-Scripts

AI-Scripts can be installed on a device running Junos OS in the following two ways:

- Automatically (recommended): Using the Junos Space Script Management feature, AI-Scripts can be installed on multiple devices simultaneously. For more information about automatically installing AI-Scripts, see [“Adding a Script Bundle to Service Now” on page 121](#).
- Manually: AI-Scripts can be installed manually on one device at a time. For more information about manually installing AI-Scripts to devices, see [“Manually Installing AI-Scripts on Devices” on page 29](#).

AI-Scripts System Requirements

AI-Scripts can be installed and run on devices running Junos OS Release 9.3 or later. For the latest AI-Scripts information, see the *AI-Scripts Release Notes*.



NOTE: The `nocopy, un-link` option is not valid when installing AI-Scripts on EX Series devices because the package is automatically deleted from the copied location of the device.

- [Downloading AI-Scripts Install Packages and Release Notes on page 27](#)
- [AI-Scripts Install Package Versioning on page 28](#)
- [AI-Scripts Install Locations on Devices on page 29](#)
- [Automatically Installing AI-Scripts Bundles on page 29](#)
- [Manually Installing AI-Scripts on Devices on page 29](#)

Downloading AI-Scripts Install Packages and Release Notes

AI-Scripts are released in AI-Scripts install packages. AI-Scripts install packages are available for download from the AI-Scripts download site. Download also the *Advanced Insight Scripts (AI-Scripts) Release Notes*.

To download an AI-Scripts install package:

1. Open a Web browser and go to the following location:

<http://www.juniper.net/support/products/serviceautomation/>.

2. Log in to the Juniper Networks authentication system using the username and password provided by Juniper Networks. To download the software, you must have a service contract and an access account. If you do not have an access account, complete the registration form at the Juniper Networks website, <https://www.juniper.net/registration/Register.jsp>.
3. Download the AI-Scripts install package.

If you are installing an AI-Scripts manually, move AI-Scripts Install Package to the `/var/sw/pkg` directory on the device. If you do not move the AI-Scripts install package to the device, you have to use FTP or Secure Copy Protocol (SCP) in conjunction with the **request system scripts add** command.

If you are installing AI-Scripts automatically on a group of devices, download AI-Scripts install Package to the same server as the Junos Space Network Management Platform software.

AI-Scripts Install Package Versioning

AI-Scripts install packages are versioned as follows:

`jais-m.nZx.x-signed.tgz`

For example:

`jais-1.0R1.5-signed.tgz`

where,

- *m.n* are two integers that represent the software release number; *m* denotes the major release number and *n* the minor release number.
- *Z* is a capital letter that indicates the type of software release. In most cases, it is R, to indicate that this is a released software. If you are involved in testing prereleased software, this letter might be B for beta-level software.
- *x.x* is the software build number and spin number.

The AI-Scripts files in the install package are compressed into a tgz tarball file.

Each AI-Scripts install package supports up to 3 previous years of Junos OS software releases.

The **show version** CLI operational command displays the version of the AI-Scripts install package that is installed on a device.

The JMB contains the output of the **show version** CLI command to indicate the version of the AI-Scripts install package installed on a device.

Refer to the *AI-Scripts Release Notes* for the current release information.

AI-Scripts Install Locations on Devices

AI-Scripts are installed on a device hard disk at the following location:

`/var/db/scripts/`

AI-Scripts are installed on a device flash drive at the following location:

`/config/scripts`



NOTE: If you configure the `load-scripts-from-flash` option, the system reads event-scripts from `/config/scripts/` directory. Otherwise, the system reads AI-Scripts from the `/var/db/scripts/` directory. The `/var/run/scripts` directory always points to the correct scripts directory.

Automatically Installing AI-Scripts Bundles

You can optionally use Service Now to install AI-Scripts bundles (also known as AI-Scripts install packages) on devices as long as there is a Junos Space Network Management Platform (Junos Space) installation. Service Now communicates with Junos Space to install AI-Scripts bundles on Junos OS devices managed by Junos Space Network Management Platform. For information about using Service Now to install AI-Scripts bundles, see [“Adding a Script Bundle to Service Now” on page 121](#).

If you do not want to use Service Now to install AI-Scripts bundles, you can manually configure and install AI-Scripts bundles to each device separately.

Manually Installing AI-Scripts on Devices

AI-Scripts can be installed on Junos OS devices manually using CLI mode. For manual installation of AI-Scripts on devices, you require the same login credentials that you use to discover devices in Junos Space.

To install AI-Scripts manually:

1. Copy the AI-Scripts install package (example: `jais-2.1R2.0-signed.tgz`) to the Junos OS device using SCP or FTP.
2. From configuration mode, execute the following commands:
`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 event-options destinations juniper-aim archive-sites /var/tmp/`
3. Install the AI-Scripts bundle install package in CLI mode using the command **`request system scripts add <full-path>/jais-2.1R2.0-signed.tgz`**.

The AI-Scripts install package is installed on the device.



NOTE: When you install AI-Scripts in the Juniper Networks QFX3000 device, ensure that you install the events scripts only on the controller. The controller installs AI-Scripts on the node devices and enables all the events.

**Related
Documentation**

- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Adding a Script Bundle to Service Now on page 121](#)

PART 2

Junos Space Service Now

- [Service Now Overview on page 33](#)
- [Using the Service Now Getting Started Assistant on page 53](#)
- [Trouble Ticket APIs Supported by Service Now on page 55](#)
- [Administration on page 71](#)
- [Service Central on page 155](#)

CHAPTER 3

Service Now Overview

- [Service Now Overview on page 34](#)
- [Upgrading Service Now on page 39](#)
- [Service Now MIBs on page 42](#)
- [Service Now Modes on page 42](#)
- [Service Now Dashboard and Workspaces Overview on page 45](#)
- [Service Now Inventory Pages on page 48](#)
- [User Roles on page 51](#)

Service Now Overview

- [Service Now Overview on page 34](#)
- [Service Now Domain on page 37](#)

Service Now Overview

Service Now is an application that runs on the Junos Space Network Management Platform to automate fault management and accelerate issue resolution. It significantly reduces the resolution time by automating support processes and using device diagnostics for fault monitoring and case automation. Your contract with Juniper Networks determines whether Service Now operates in standard mode, partner-proxy mode, end-customer mode, or offline mode. These modes in turn determine which tasks are enabled and disabled in Service Now. For information on Service Now modes, see [“Service Now Modes” on page 42](#).

To help ensure maximum network uptime, AI-Scripts installed on devices automatically detect and report incidents to Service Now. An incident is the occurrence of a defined event such as a process crash, an application-specific integrated circuit (ASIC) error, or a fan failure. When an incident is detected in devices with AI-Scripts enabled, AI-Scripts automatically collect diagnostic data and package it into a file called a *Juniper Message Bundle* (JMB). JMBs contain comprehensive information about the device identity, the problem event, and diagnostics. This information is securely transferred to the Junos Space platform. Service Now then notifies users about the new incident by sending an e-mail or an SNMP trap.

In addition to reporting incidents, AI-Scripts also collect device information regularly in the form of *Information Juniper Message Bundles* (iJMBs). The iJMBs are generated once in seven days.

In Service Now, JMB errors are JMBs that do not comply with the standard data structure that is expected by Service Now or that contain unexpected data elements. Service Now identifies these JMBs and displays them on the JMB Errors page, where they can be viewed and downloaded.

After reviewing information provided in the JMB, you can submit the incidents to Juniper Support Systems (JSS) to create a Juniper Networks Technical Assistance Center (JTAC) case. The case is processed and analyzed to provide faster analysis and alerts. Using Service Now, you can track the status of the case. To restrict the amount of information you share with Juniper Networks, you can filter configuration content from iJMBs before submission.

Apart from submitting JMBs to obtain resolutions, you can use Service Now to perform the following tasks:

- assign an owner (user) to a reported incident
- flag users to keep them notified of the changes made to the incident
- set up notification policies for users who need to be kept informed of changes to incidents that affect them

- update the incident status
- delete JMBs from the Service Now database
- export data in the incident and information messages to HTML, CSV, and Excel and store in the local file system

To add multiple devices and organizations, you need to obtain a technical support contract with the right level of service. After you have a valid contract, you can submit incidents and iJMBs to JSS for support. Without a valid contract, Service Now runs in demo mode and supports one organization and five devices for 60 days. In this mode, you cannot connect to JSS or open technical support cases with JTAC.

To open technical support cases and share iJMBs with Juniper Networks, you must first set up an organization in Service Now. An organization represents a unique Clarify site ID in JSS that is used to identify customers while providing technical support. After creating an organization, you can test its connectivity with JSS and even set the submission of incidents as test cases. If you are a Juniper Networks partner or a direct customer with multiple distinct networks, you can use multiple Service Now organizations to keep customers or networks separate.

You can group network elements and manage multiple devices as a single entity using Service Now device groups. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Device groups help you regulate access to Service Now devices. After you add devices and create device groups, you can perform various operations on them, such as installing or removing AI-Scripts individually on every device or on all the devices in a device group simultaneously. You can even edit their parameters and delete them from the Service Now database.

Service Now partner proxy lets you display the state of an end-customer device after it is added or removed by a connected member.

Connected-member devices are added to the partner proxy in two scenarios:

- When a case is submitted from an end customer to the partner proxy
- When an iJMB is uploaded from an end customer to the partner proxy

In both the scenarios, a notification is triggered from the partner proxy.

When a device is removed by a connected member, a notification is sent to the partner proxy. In case a removed device (that is still present in the partner proxy in Removed state) is added again by a connected member, a notification is sent to partner proxy with the changed state. The partner proxy will update the device state from Removed to Added if the device is already present in the partner proxy and triggers a notification. If the device does not exist in the partner proxy, no action will be performed.

In addition to monitoring and managing devices, organizations, and device groups, you can incorporate the use of SNMP and proxy servers. SNMP servers act as destinations where traps are sent when a notification policy is triggered. Configuring Service Now to work with a proxy server facilitates all communication to and from JSS through the proxy server, ensuring secure transactions.

The Service Now dashboard displays the gadgets and the workspaces that the user can use to perform various tasks. For more information about the Service Now dashboard and icons, see “[Service Now Dashboard Overview](#)” on page 45.

To install, upgrade, and remove Service Now, you need Junos Space administrator privileges. *Adding a Junos Space Application and Uninstalling a Junos Space Application* in the *Junos Space Network Management Platform User Guide* at http://www.juniper.net/techpubs/en_US/junos-space2.0/information-products/topic-collections/junos-space-network-application-platform-pwp/junos-space-network-application-platform-pwp.pdf. You can install, remove, or upgrade Service Now even while Junos Space and Junos Space applications are still running.

With different Service Now user privileges, you can perform one or more of the following tasks:

- Add devices to Service Now from the Junos Space platform
- Add or delete a script bundle
- Install or remove AI-Scripts on devices
- Add, modify, or delete devices and device groups
- Associate devices with device groups
- Add, modify, or delete an organization
- Submit incidents as test cases
- Test organization connectivity to JSS
- Export device data in CSV and Excel formats
- View information about devices that risk the chance of exposure
- Export inventory information in CSV and Excel formats
- Configure the global settings (SNMP server and proxy server settings)
- Share information with Juniper about Service Now Incidents and Service Now Devices
- Assign an owner, flag to users, update status of incidents, and delete incidents
- View and delete iJMBs, and export device data into HTML format
- Assign an owner, notify users, and delete an information message
- View, download, and delete JMBs with errors
- Create, edit, and delete a notification policy

**Related
Documentation**

- [Service Central Overview on page 155](#)
- [Administration Overview on page 71](#)
- [Service Now Domain on page 37](#)

Service Now Domain

A domain is a logical grouping of objects in Junos Space. A Junos Space administrator creates and manages domains in the Junos Space Network Management Platform. For more information about domains, see *Junos Space Network Management Platform User Guide* at [Junos Space Network Management Platform Documentation](#).

A device is assigned to a domain in the Junos Space Network Management Platform. When the device is added to Service Now, the device continues to belong to the domain to which it is assigned in the Junos Space Network Management Platform. Service Now objects such as incidents, device snapshots, error JMBs, and support cases that are related to the device are assigned to the same domain as the device.

When you log in to Service Now, objects such as organization, script bundle, SNMP configuration, and Email template, which are assigned to the domain that you are currently in, and the objects in the system domain are visible to you. If you are assigned to more than one domain, you can access the other domains and objects in those domains by selecting the domains from the **Login as username in** list. Only the domains to which you are assigned are listed. A super user can access all domains.

Objects that you create when you are logged in to a certain domain are assigned to that domain. However, if you have administrative privileges, you can assign the objects to another domain. For information about changing the domain of an object, refer to [“Assigning a Service Now Object to Another Domain” on page 39](#).

Objects such as script bundles, SNMP configurations, and Email templates that are used by objects in all domains are assigned to the system domain. Objects assigned to the system domain are visible in all domains.

You cannot modify the domain of Service Now devices and the objects such as incidents, error JMBs, device snapshots, and support cases related to the Service Now devices. However, you can modify the domain of devices of end customers. The devices of end customers are, by default, present in the domain assigned to them by the connected member.

When the device is assigned to a domain, objects such as technical or end-customer support cases that are not assigned to any device belong to the domain assigned to the organization associated with the device. [Table 3 on page 38](#) lists Service Now objects and their default domains.

Table 3: Service Now Objects and Their Default Domains

Service Now Objects	Default Domain	
	Fresh Installation	Migration
<ul style="list-style-type: none"> • Organization • Connected Member • Device Group • Address Group • Notification • Auto Submit Policy • Event Profile • Product Health Data Configuration 	Domain to which a user is logged in	Global domain
<ul style="list-style-type: none"> • Global Setting • SNMP Configuration • Core File Upload Configuration • Message • Script Bundle • Email Template • End Customer Information Message • Script Installation Advisor (SIA) 	System domain	System domain
<ul style="list-style-type: none"> • Service Now Device • Incident • Device Snapshot • Error JMB • Technical Support Case • End Customer Case 	Domain assigned to the device in Junos Space Network Management Platform	Domain assigned to the device in Junos Space Network Management Platform

Assigning a Service Now Object to Another Domain

If you are assigned to multiple domains, you can assign an object from the domain that you are currently in to another domain to which you are assigned. All objects except objects in the system domain can be assigned to another domain.

To assign a Service Now object to another domain:

1. From the Service Now navigation tree, select the object.

The object's landing page appears.

2. On the landing page, select the object's instance that you want to assign to another domain.

You can also select multiple instances of the object to assign to another domain.

3. From the Actions menu, select **Assign object to domain**. Alternatively, right-click the object and select **Assign object to domain**.

The Assign to Domain dialog box appears.

4. Under Assign selected items to domain, select the domain and click **Assign**.

The Assign to Domain dialog box closes and the object is not listed on the object's page.

5. From the **Login as username** in list, select the domain to which you assigned the object.

The Service Now GUI is refreshed.

6. Using the Service Now navigation tree, open the object's page and check whether the object is listed on the page.

Related Documentation

- [Service Central Overview on page 155](#)
- [Administration Overview on page 71](#)
- [Managing Domains Overview](#)

Upgrading Service Now

- [Upgrading Service Now on page 39](#)

Upgrading Service Now

You can upgrade Service Now to up to two versions later than its current version. For example, Service Now version 1.2 can be upgraded to versions 1.3 or 1.4. To upgrade from Service Now version 1.2 to a version later than 1.4, you must first upgrade to version 1.4 and then upgrade again to the required version.



NOTE: Service Insight is automatically upgraded along with Service Now.

You can upgrade Service Now and Service Insight in one of the following ways:

- As part of the Platform upgrade: When you upgrade the Junos Space Platform, Junos Space determines the running versions of the Service Now and Service Insight applications, and upgrades them to the latest versions. If the running versions are the latest, then Junos Space continues with the rest of the Platform upgrade without upgrading Service Now or Service Insight.

For information on upgrading the Platform, see *Upgrading Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide*.

- As a separate application: You can upgrade Service Now and Service Insight together as a separate hot-pluggable application.

To upgrade Service Now and Service Insight together as a separate hot-pluggable application:

1. Ensure that the image to which you want to upgrade is downloaded to the local client file system using <https://www.juniper.net/support/products/space/#sw>.

2. Click **Network Management Platform > Administration > Applications**.

The Applications inventory page appears.

3. In the workarea, select **Service Now**, and click **Upgrade Application** from either the **Actions** list or the right-click menu.

The Upgrade Service Now appears and displays all previously uploaded versions of the applications.

4. Do one of the following:

- If the application that you want to upgrade is listed in the Upgrade Application dialog box, select the file, and click **Upgrade**.

The application upgrade process begins. (Go to 5.)

- If the application that you want to upgrade is not listed in the Upgrade Application dialog box, click **Upload**.

The Software File page appears. For information on how to upload the application, go to 1.

5. You enter maintenance mode. Junos Space prompts you to enter a username and password to enter maintenance mode. The username is **maintenance**; the password is the one that the administrator created during the initial installation process.
6. Enter the maintenance mode username and password in the text field.
7. Click **OK**.

Junos Space displays a status window during the upgrade process.

8. When the Service Now upgrade finishes, a message appears confirming that Service Now is successfully upgraded.



NOTE: The upgrade process takes between 2 and 30 minutes to finish depending on the size of the Junos Space database.

To upload a new application:

1. Select one of the following options:

- Click **Upload via HTTP**.

The **Software File** dialog box appears. Enter the application name, or click **Browse** to navigate to the new Junos Space application file on the local file system, and then click **Upload**.

- Click **Upload via SCP**.

The **Upload Software via SCP** dialog box appears. Enter the requested credentials: username, password, host IP address, and the path of the Junos OS application file. Click **Upload**.

The new applications are uploaded from the local file system into Junos Space and displayed by application name, filename, version, release level, and required Junos Space Network Management Platform version. When the process is completed, the **Upgrade Job Information** dialog box appears.

2. In the **Upgrade Job Information** dialog box, click the Job ID link to see the Upgrade Application job on the Jobs inventory page.
3. Click **Administration > Applications** to continue with the add application process.

The Applications inventory page appears.

4. Right-click the **Service Now** application and select **Upgrade Service Now**.
5. Click **OK**.

The **Upgrade Service Now** dialog box appears. You see the application file that was uploaded.

6. Select the application file to which you want to upgrade, and click **Upgrade**. The application upgrade process begins.

When you upgrade an instance of Service Now that operates in the end-customer or partner-proxy mode, ensure that the Service Now is either the same version or no more than two versions later than the end-customer Service Now applications that it connects to.

For example, as a Service Now end-customer, if you upgrade to Service Now 1.3, the Service Now that you connect to should be upgraded to Service Now version 1.3, 1.4, or 2.0. A Service Now upgraded to Service Now version 2.0 can only connect to end-customer Service Now application versions 2.0, 1.4, and 1.3.

Related Documentation

- *Upgrading Junos Space Software Overview*

Service Now MIBs

- [Service Now MIBs on page 42](#)

Service Now MIBs

Service Now supports Juniper Networks enterprise-specific management information bases (MIBs). These MIBs define the traps that Service Now sends to a remote network management system. The sent traps correspond to the trigger specified for a notification policy. For information about creating a notification policy in Service Now, see [“Creating and Editing a Notification Policy” on page 187](#).

Using Service Now notifications, you can configure Service Now to send SNMP traps to one or more of your SNMP servers. To enable an SNMP server to receive traps from Service Now, load the following MIBs in the order listed below:

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

To download these MIB files:

- From the Application Chooser, select **Service Now**. The dashboard appears, which displays the **Service Now Notices** box.
- In the **Service Now Notices** box, click the **Click here** link provided in the **To download Service Now Mibs click here** statement.

The **Technical Documentation** page opens. The Service Now MIBs are stored by release versions in this page.

- Click the respective version to download the required MIB files.

Related Documentation

- [Adding an SNMP Server on page 129](#)
- [Service Now Overview on page 34](#)

Service Now Modes

- [Service Now Modes on page 42](#)

Service Now Modes

- [Overview on page 43](#)

Overview

Depending on your contract with Juniper Networks, Service Now operates in Standard, End Customer, and Partner Proxy modes. Service Now enables and disables certain features based on its mode of operation.



NOTE: Service Now and Service Insight should be run in the same server group of a JBoss EAP domain as the Junos Space Network Management Platform. Operating Service Now, Service Insight, and Junos Space Network Management Platform in different server groups is not supported.

For information on running Junos Space applications in server groups, refer to *Junos Space Network Management Platform User Guide*.

- Demo mode—Service Now operates in demo mode from the time you install Junos Space and until you create a Service Now organization and validate the organization's connection with JSS.

In this mode, Service Now supports a single organization and up to five devices. The connection between Service Now and Juniper Support Services (JSS) is disabled, preventing the creation of technical support cases.

- Offline mode—You can accept a standalone or Partner Proxy license file and activate the Junos Space Platform and Service Now application without having to connect to the Juniper Support Service (JSS). You can perform all Service Now tasks except submit cases, create auto submit policies, view exposure, or view cases in Case Manager. You do not have the option to work in offline mode if Service Now is already in the end-customer mode.
- Standard mode—In standard mode, you can add multiple Service Now organizations and devices. Service Now is connected to JSS which enables JSS to provide support for the incidents and device snapshots that you submit.
- End-customer mode—Service Now can be operated in the end-customer mode by customers such as service providers and enterprises who want to manage their networks. In this mode, Service Now and JSS communicate through a Juniper Networks partner's Service Now application. A partner manages multiple customers using a secure HTTPS connection that is established between the customer and the partner's Service Now applications.

The partner provides credentials to a customer to create an organization. The customer creates an organization using the credentials, and submits incidents to the partner. The partner submits the cases to JSS and sends case updates back to the customer. JSS validates the customer only when an iJMB or incident is submitted to it.

Standard mode and end customer mode have similar functions; however, in the end customer mode, you can create only one organization and you submit cases to the partner instead of the JSS.

- Partner Proxy mode—Service Now can be operated in the partner-proxy mode by a qualified Juniper Networks partner. A Juniper Networks partner manages Service Now

applications of multiple customers. A secure HTTPS connection is made between the Service Now applications of every customer and the partner, as well as between the partner and JSS. The partner receives JMBs from the customers and can either submit the JMBs to JSS on behalf of the customers or handle the cases without JSS support.

In this mode, a partner can add multiple organizations and device groups and associate every customer with an organization. In the JSS, each organization is associated with a Site ID and cases from customers are opened with Juniper Networks under the site ID associated with the customer's organization. When you add a connected member, a default device group is created. You cannot delete this device group manually; however, it is automatically deleted when the connected member is deleted.

To connect to an end-customer, a Service Now partner uses a self-signed security certificate. Although this method of identification is not trusted, this certificate is automatically accepted to ensure that the communication between the partner and the customer is encrypted.

For Juniper Care Plus customers, Service Now enables Service Insight (SI) application in Standalone or Partner mode.

Table 4 on page 44 lists the tasks that are enabled for the Service Now modes.

Table 4: Tasks Enabled for Service Now Modes

Task	Demo Mode	Standard Mode	End Customer Mode	Partner Proxy Mode
Adding more than five devices	–	Enabled	Enabled	Enabled
Adding more than one organization	–	Enabled	–	Enabled
Adding connected members	–	–	–	Enabled
Updating end-customer cases	–	–	–	Enabled
Assigning messages to an end-customer	–	–	–	Enabled
Viewing messages assigned to an end-customer	–	–	–	Enabled
Creating technical Support Cases	–	Enabled	–	Enabled
Installing and removing AI-Scripts on devices	Enabled	Enabled	Enabled	Enabled (only for partner's devices)
Other tasks	Enabled	Enabled	Enabled	Enabled

- Related Documentation**
- [Administration Overview on page 71](#)
 - [Service Central Overview on page 155](#)
 - [Configuring Global Settings on page 123](#)
 - [Adding an Organization on page 75](#)
 - [Adding a Connected Member on page 77](#)

Service Now Dashboard and Workspaces Overview

- [Service Now Dashboard Overview on page 45](#)

Service Now Dashboard Overview

The Service Now dashboard displays notifications and graphs about platforms and devices with most incidents. You can view the Service Now dashboard by selecting **Service Now** from the Application Chooser.

The Service Now dashboard includes:

- [Service Now Workspaces on page 45](#)
- [Dashboard Gadgets on page 46](#)

Service Now Workspaces

Apart from the Service Central and Administration workspaces, Service Now also provides shortcuts to the Devices and Jobs workspaces by including them in the Service Now navigation tree.

For more details, refer to the *Junos Space Network Management Platform User Guide*.

You can perform the following tasks from the **Jobs** workspace:

- View status of all scheduled, running, canceled, and completed jobs
- Retrieve details about the execution of a specific job
- View statistics about the average execution times for jobs, types of jobs that are run, and success rate
- Cancel a scheduled job or in-progress job when the job is stalled and is preventing other jobs from starting
- Archive old jobs and purge them from the Junos Space Network Management Platform database
- Retry a job on failed devices on Service Now and Service Insight. The action **Retry on Failed Devices** is available for the following jobs:
 - Failed event profile installation
 - Failed event profile un-install
 - Failed create on-demand incident job

For retrying jobs on failed devices, see [Retrying a Job on Failed Devices](#) from the *Junos Space Network Management Platform user Guide*.

[Table 5 on page 46](#) lists the tasks that can be performed using the Service Now workspaces.

Table 5: Service Now Workspaces

Workspace Name	Tasks
Service Central	<ul style="list-style-type: none"> • Assign an incident to a user to take the ownership, notify users about the incident, update the status of incidents, and delete incidents. • View and delete JMBs, and export device data into HTML format. • Deliver messages from JSS to customers (enabled if you are a Juniper Networks partner and working in partner-proxy mode). • Update customer cases (enabled if you are a Juniper Networks partner and working in partner-proxy mode). • View, download, and delete JMBs with errors from the Service Now database. • View Knowledge Base (KB) articles associated with incidents. • View information about devices that risk the chance of exposure. • Assign an owner, flag to users, and delete an information message. • Create, edit, and delete a notification policy.
Administration	<ul style="list-style-type: none"> • Add devices to Service Now from the Junos Space platform. • Add or delete an event profile or a script bundle. • Add and delete devices and device groups. • Install or remove AI-Scripts on devices. • Associate devices with device groups. • Add, modify, or delete an organization. • Add connected members and view messages assigned to them (enabled if you are a Juniper Networks partner and working in partner-proxy mode). • Create organizations in test mode and test the connectivity between the organization and JSS. • Export device data in CSV and Excel formats. • Export inventory information in CSV format. • Configure the global settings (SNMP server and proxy server settings). • A client can associate address location to devices, and a user can associate a device location or a ship-to-address to a device. • Modify E-mail templates.

Dashboard Gadgets

The Service Now dashboard displays gadgets (graphs and charts) with information that is updated automatically. You can move the gadgets on the dashboard and change their

sizes. These changes persist even after you log out of the system. The gadgets displayed on the Service Now dashboard are:

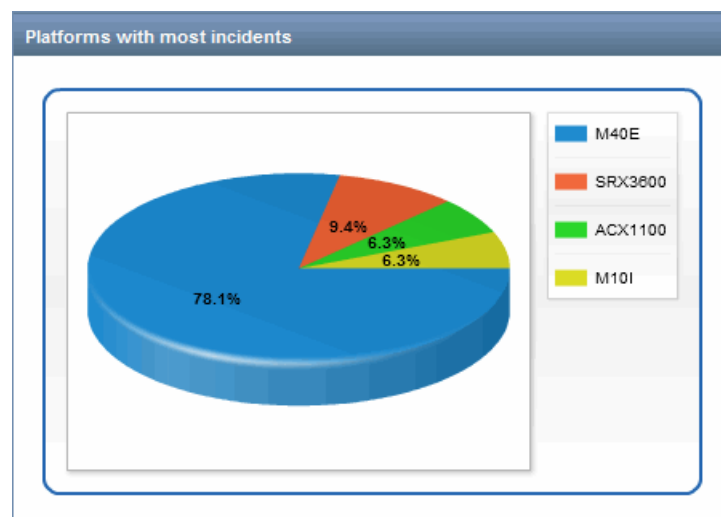
- [Platforms with Most Incidents on page 47](#)
- [Devices with the Most Incidents on page 47](#)
- [Service Now Notices \(Upgrade and Contract Notice\) on page 48](#)

Platforms with Most Incidents

This gadget graphically displays the platforms with the most incidents and the percentage of incidents detected on them. Clicking the elements within the graph takes you to the Incidents page, where incidents are filtered to display only the incidents that occurred on the platform that you clicked.

For example, when you click the **ACX1100** element in the **Platforms with most incidents** gadget (as shown in [Figure 2 on page 47](#)), the Incidents page displays only those incidents that are detected on the ACX1100 router.

Figure 2: Platform with Most Incidents Gadget

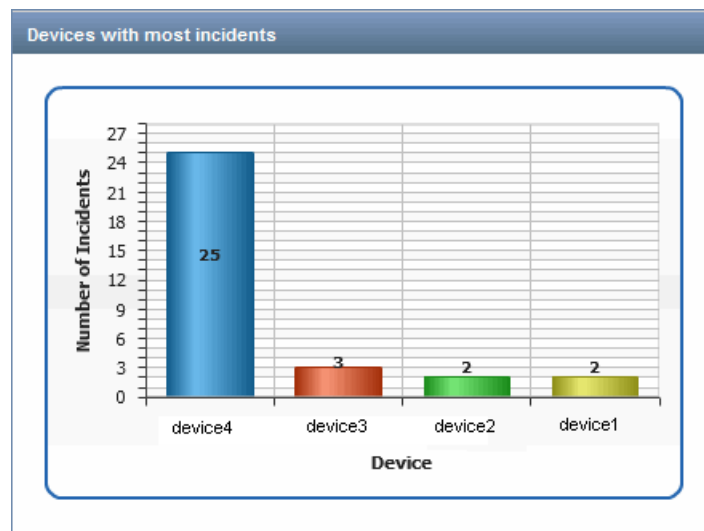


Devices with the Most Incidents

This gadget displays the devices with the most incidents graphically, along with the number of incidents detected on them. Clicking the elements within the graph takes you to the Incidents page, where incidents are filtered by the device category. You see only the incidents that affect the device that you selected. You can filter the incidents on the Manage Incidents page according to your selection on this graph. To do this, click the **Devices** bar of your choice in the graph to take you to the Manage Incidents page, which displays only those incidents that affect the device that you selected.

As shown in [Figure 3 on page 48](#), clicking **device1**, which is represented by the yellow bar of the graph, displays the Incidents page where incidents are filtered to display only those incidents that occurred on antlia.

Figure 3: Devices with Most Incidents Gadget

**Service Now Notices (Upgrade and Contract Notice)**

This gadget notifies you about the tasks that you need to execute after a Junos Space upgrade. It also informs you about your contract with Juniper Networks.

Related Documentation

- [Service Central Overview on page 155](#)
- [Administration Overview on page 71](#)
- [Service Now Icons and Inventory Pages](#)

Service Now Inventory Pages

- [Filtering Inventory Pages on Service Now and Service Insight on page 48](#)

Filtering Inventory Pages on Service Now and Service Insight

All the inventory pages provide column based filtering so that you can filter data by a specific column. The filters are present in the drop-down list of the columns. The drop-down list has an input field where you can enter the filter criteria. On applying the filters, the table contents display values that match the applied filter criteria.

Depending on the table, different columns can be filtered on. [Table 6 on page 49](#) lists the tables that permit filtering.

Table 6: Filter-enabled Tables and Columns

Work-space	Page / Table	Columns
Administration	Organizations	All columns except: <ul style="list-style-type: none"> • Submit Cases As
	Device Groups	All columns
	Service Now Devices	All columns except: <ul style="list-style-type: none"> • Connected Member • Ship-to • Location • Policy
	Event Profiles	All columns except: <ul style="list-style-type: none"> • Devices
	Script Bundles	All columns
	Auto Submit Policy	All columns except: <ul style="list-style-type: none"> • Events • Devices • Incident Submitted
	Address Group	All columns except: <ul style="list-style-type: none"> • Devices
	E-mail Templates	All columns except: <ul style="list-style-type: none"> • Description

Table 6: Filter-enabled Tables and Columns *(continued)*

Work-space	Page / Table	Columns
Service Central	Incidents	All columns except: <ul style="list-style-type: none"> • Connected Member • Total Core Files • Flag
	View Tech Support Cases	All columns except: <ul style="list-style-type: none"> • Organization • Time Created
	View End Customer Cases	All columns
	Information messages	All columns except: <ul style="list-style-type: none"> • Organization
	Device Snapshots	All columns except: <ul style="list-style-type: none"> • Connected member
	JMB Errors	All columns
	Notifications	All columns
Insight Central	Exposure Analyzer	All columns except: <ul style="list-style-type: none"> • Connected Member
	EOL Reports	All columns except: <ul style="list-style-type: none"> • Devices selected
	PBN Reports	All columns except: <ul style="list-style-type: none"> • Devices selected
	Targeted PBNs	All columns
	Notifications	All columns

For procedure regarding filtering inventory pages, see *Filtering Inventory Pages* section from the *Junos Space Network Management Platform User Guide*.

Related Documentation

- [Service Now Overview on page 34](#)
- [Table 21 on page 202](#)

User Roles

- [Service Now User Roles on page 51](#)

Service Now User Roles

The Junos Space administrator creates users and assigns roles (permissions) that allow you to access and perform different tasks. You cannot view the tasks that you do not have access to. While Junos Space allows creating users with custom permissions, it also has a set of predefined user roles. These predefined roles cannot be modified or deleted. See [Table 7 on page 51](#), for the list of predefined user roles available in Service Now.

To create and manage users, select **Application Switcher > Network Management Platform > Users > Manage Users**. The Manage Users page lists the existing users. Use this page to create and assign roles to Service Now users.

You can also navigate to the Manage Users page by selecting **Application Switcher > Jump to Users**.

Table 7: Predefined Service Now User Roles and Permissions

Role	Permitted to Execute Actions Under the Following Subtasks	
Service Now Admin	Administration	Service Now Devices, New Device Platform Event Profiles, Add Event Profile Script Bundle, Add Script Bundle Organization, Add Organization, Add member Global Settings, SNMP Configuration, Manage SNMP Traps, Proxy Server Configuration Device Group, Create Device Group View Auto Submit Policy, Create Auto Submit Policy Address Group, Create Address Group E-mail Templates
	Service Central	Incidents, View Tech Support Cases JMB Errors Information, Messages, Device Snapshots Notifications, Create Notification

Table 7: Predefined Service Now User Roles and Permissions (*continued*)

Role	Permitted to Execute Actions Under the Following Subtasks	
Service Now Unrestricted User	Administration	Service Now Devices
	Service Central	Incidents, View Tech Support Cases
		JMB Errors
		Information, Messages, Device Snapshots
		Notifications, Create Notification
		Permissions exclude the ability to delete managed objects
Service Now Read Only User	Administration	Viewing and exporting Service Now devices
	Service Central	Viewing JMB details
		Exporting incident summary into an Excel format
		Viewing an incident case in the Case Manager
		Viewing a technical support case in Case Manager
		View end-customer cases in Case Manager
		Downloading JMB errors
		Scanning an information message for impact
		Exporting a JMB (device snapshot) to HTML
		Viewing JMB (device snapshot) details
		Viewing notification policies

You can flag or assign an incident only to a Service Now Admin or Service Now Unrestricted User. You can flag or assign an information message or iJMB to any user. Regardless of the permissions you have, you can always clear a flag of an incident or information message that had been flagged to you.

Related Documentation

- [Service Central Overview on page 155](#)
- [Administration Overview on page 71](#)

CHAPTER 4

Using the Service Now Getting Started Assistant

- [Service Now Getting Started Assistant Usage Overview on page 53](#)

Service Now Getting Started Assistant Usage Overview

- [Service Now Getting Started Assistant Usage Overview on page 53](#)

Service Now Getting Started Assistant Usage Overview

The Getting Started assistant is a sections in the Junos Space sidebar that guides you through the tasks that you can perform as part of the initial setup for every application. It appears when you log in to Junos Space and the **Show Getting Started on Startup** check box is selected.

To use the Service Now Getting Started assistant, navigate to Service Now, click the **Help** icon, expand the **Getting Started** assistant, and click the **Initial Setup** link. The **Getting Started** assistant displays five required steps and one optional step.

Every step in the Getting Started assistant contains a task link, and alongside the task links are help icons that provide information about the individual tasks. To execute the steps, click the task links of every step. The inventory page displays the page where you can execute the tasks.

By default, the Getting Started assistant guides you through the steps required to set up standard mode for Service Now.

The following steps are required:

1. Review Global Settings.
See [“Configuring Global Settings” on page 123](#)
2. Create Organization.
See [“Adding an Organization” on page 75](#).
3. Add Devices to Junos Space.
See the *Discovering Devices* section of the *Junos Space Network Management Platform User Guide*.
4. Create Device Group.

See [“Creating a Device Group” on page 83](#).

5. Install Scripts using Service Now Devices.

See [“Installing an Event Profile on Devices Using Service Now” on page 91](#)

The following step is optional:

- Add New Script Bundle.

See [“Adding a Script Bundle to Service Now” on page 121](#).

To activate Service Now in end-customer and partner-proxy modes, see the Activating the End-Customer and Partner-Proxy Modes section in [“Service Now Modes” on page 42](#).

**Related
Documentation**

- [Service Now Overview on page 34](#)

CHAPTER 5

Trouble Ticket APIs Supported by Service Now

- [Trouble Ticket APIs Overview on page 55](#)
- [Profiles Used by Service Now on page 56](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)

Trouble Ticket APIs Overview

Service Now supports trouble ticket APIs that allow you to perform the following functions:

- Create, query, close, or cancel trouble tickets (single/multiple)
- Change the values of trouble tickets (single/multiple)
- Obtain notification regarding ticket changes

The Operation Support Systems for Java (OSS/J) delivers standards-based interface implementations (OSS/J APIs) and design guidelines for the development of component-based OSS systems. The web service technology is used to expose the standard set of APIs defined under JSR91 of OSS/J. The OSS/J module is integrated into Service Now. For more details, refer to the JSR 91 specification at <http://www.tmforum.org/>.

The version of the trouble ticket supported by Service Now is TroubleTicket_x790/v0-5.

Related Documentation

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Setting up Java Based Web Service Client on page 56](#)

- [Profiles Used by Service Now on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

Profiles Used by Service Now

A profile in OSS through Java is equivalent to an interaction pattern. A profile describes how a client can interact with the OSS/J application.

Currently, Service Now supports the Web Services style interaction profile (WSIP) for displaying trouble ticket APIs to clients. The reason for choosing Web Services is its ability to enable different systems to communicate at the protocol level without requiring any specific agreement on middleware, software libraries, programming languages, component models, application server platforms, processors or operating systems.

WSIP relies on well established standards such as SOAP (Simple Object Access Protocol) and WSDL (Web Services Description Language).

Related Documentation

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

Setting up Java Based Web Service Client

To set up a java based web service client:

1. Download the WSDL and XSD files from Service Now server [https://\[IP address\]/aimOSSTroubleTicketService/OSSJWSDLFile?baseURL=https://\[IP Address\]/aimOSSTroubleTicketService/JVTTroubleTicketWS](https://[IP address]/aimOSSTroubleTicketService/OSSJWSDLFile?baseURL=https://[IP Address]/aimOSSTroubleTicketService/JVTTroubleTicketWS) , where IP address is the IP address of the Service Now host.
2. Download the OSSJWSDLAndXSDFiles.zip file containing the WSDL and XSD files. Extract the zip files to the required location.

The zip file contains the following files:

- JVTTroubleTicketSession.wsdl
- WS-BaseNotification.wsdl
- WS-Resource.wsdl

- License.xml
 - xsd/notification/b-2.xsd
 - xsd/notification/bf-2.xsd
 - xsd/notification/r-2.xsd
 - xsd/notification/t-1.xsd
 - xsd/notification/ws-addr.xsd
 - troubleTicket/OSSJ-Common-v1-5.xsd
 - troubleTicket/OSSJ-Common-CBEBi-v1-5.xsd
 - troubleTicket/OSSJ-Common-CBECORE-v1-5.xsd
 - troubleTicket/OSSJ-Common-CBEDatatypes-v1-5.xsd
 - troubleTicket/OSSJ-Common-CBELocation-v1-5.xsd
 - troubleTicket/OSSJ-Common-CBEParty-v1-5.xsd
 - troubleTicket/OSSJ-Common-SharedAlarm-v1-5.xsd
 - troubleTicket/OSSJ-TroubleTicket-CBETrouble-v1-2.xsd
 - troubleTicket/OSSJ-TroubleTicket-v1-2.xsd
 - troubleTicket/OSSJ-TroubleTicket_x790-v0-5.xsd
3. In a windows system, select **START** > **RUN** to open the command prompt. Type **cmd** in the Run dialog box, and then press **OK**. Navigate to the location where the zip file has been extracted.
 4. Navigate to the location where the zip file is extracted and run the following command to generate the service Now OSS/J web service client binaries: **wsimport -d [LOCATION_FOR_CLIENT_BINARIES] JVTTroubleTicketSession.wsdl**. where *LOCATION_FOR_CLIENT_BINARIES* is the location to generate the web service client.

Example— OSSJTroubleTicketClient.java:

```
import java.lang.reflect.Field;
import java.lang.reflect.InvocationTargetException;
import java.lang.reflect.Method;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.List;

import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import javax.xml.bind.JAXBElement;
import javax.xml.ws.BindingProvider;
import javax.xml.ws.handler.Handler;
```

```
import org.apache.xerces.jaxp.datatype.DatatypeFactoryImpl;
import org.ossj.wsdm.troubleshoot.v1_2.JVTTroubleTicketSessionWSPort;
import org.ossj.wsdm.troubleshoot.v1_2.JVTTroubleTicketSessionWebService;
import org.ossj.xml.common.ArrayOfString;
import org.ossj.xml.troubleshoot.v1_2.*;

public class OSSJTroubleTicketClient {

    public static void main(String[] args) {
    try {

        //create web service client object
        JVTTroubleTicketSessionWebService webService1 = new

                                JVTTroubleTicketSessionWebService();
        //get the port from the webservice client

        JVTTroubleTicketSessionWSPort port =
        webService1.getJVTTroubleTicketSessionWSPort();
        //disable SSL certificate verification - this will be needed when using HTTPS server.
        disableCertificateValidation();

        //Authentication data must be added into SOAP request, for this creating a handler
        //chain which adds the authentication in SOAP header of the outgoing message.
        //The handler chain is then associated with the webservice port
        List<Handler> handlerChain = new ArrayList<Handler>();
        handlerChain.add(new SOAPLoggingHandler());
        BindingProvider bindingProvider = (BindingProvider) port;
        List<javax.xml.ws.handler.Handler> ls =
            bindingProvider.getBinding().getHandlerChain();
        ls.add(new SOAPLoggingHandler());
        bindingProvider.getBinding().setHandlerChain(handlerChain);

        //create request for creating trouble ticket
        CreateTroubleTicketByValueRequest request = createTroubleTicketValueRequest();

        //invoke the createTroubleTicketByValue API
        CreateTroubleTicketByValueResponse response =
        port.createTroubleTicketByValue(request);

    } catch (Exception e) {
        e.printStackTrace();
    }
    }

    public static void disableCertificateValidation() {
    // Create a trust manager that does not validate certificate chains
    TrustManager[] trustAllCerts = new TrustManager[] {
        new X509TrustManager() {
            public X509Certificate[] getAcceptedIssuers() {
                return new X509Certificate[0];
            }
        }
    };
    }
```

```

    }
    public void checkClientTrusted(X509Certificate[] certs, String authType) {}
    public void checkServerTrusted(X509Certificate[] certs, String authType) {}
  };
  // Ignore differences between given hostname and certificate hostname
  HostnameVerifier hv = new HostnameVerifier() {
    public boolean verify(String hostname, SSLSession session) { return true; }
  };

  // Install the all-trusting trust manager
  try {
    SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(null, trustAllCerts, new SecureRandom());
    HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFactory());
    HttpsURLConnection.setDefaultHostnameVerifier(hv);
  } catch (Exception e) {}
}

private static CreateTroubleTicketByValueRequest createTroubleTicketValueRequest()
{
  TroubleTicketValue value = new ObjectFactory().createTroubleTicketValue();

  //set the values in TroubleTicketValue object

  CreateTroubleTicketByValueRequest request = new
    ObjectFactory().createCreateTroubleTicketByValueRequest();

  request.setTroubleTicketValue(value);

  return request;
}
}

```

Example—SOAPLoggingHandler.java

```

import java.io.ByteArrayOutputStream;
import java.util.Set;
import java.util.logging.Logger;

import javax.xml.namespace.QName;
import javax.xml.soap.SOAPElement;
import javax.xml.soap.SOAPException;
import javax.xml.soap.SOAPHeader;
import javax.xml.soap.SOAPEnvelope;
import javax.xml.soap.SOAPMessage;
import javax.xml.ws.handler.MessageContext;
import javax.xml.ws.handler.soap.SOAPHandler;
import javax.xml.ws.handler.soap.SOAPMessageContext;

public class SOAPLoggingHandler implements SOAPHandler<SOAPMessageContext>
{
  private static Logger logger =

```

```
Logger.getLogger(SOAPLoggingHandler.class.getName());

    public boolean handleMessage(SOAPMessageContext context) {
        Boolean outGoingMsg = (Boolean)
context.get(MessageContext.MESSAGE_OUTBOUND_PROPERTY);
        SOAPMessage soapMsg = context.getMessage();

        if(soapMsg != null && soapMsg.getSOAPPart() != null) {

            SOAPEnvelope soapEnv;

            try {
                soapEnv = soapMsg.getSOAPPart().getEnvelope();
                SOAPHeader soapHeader = soapEnv.getHeader();
                if (soapHeader == null) {
                    soapHeader = soapEnv.addHeader();
                }

                addAuthentication(soapHeader);
            } catch (SOAPException e) {
                // TODO Auto-generated catch block
                e.printStackTrace();
            }
        }

        if (outGoingMsg)
            System.out.println("#####outgoing soap message#####");
        else
            System.out.println("#####incoming soap message#####");

        logSoapMessage(context);

        return true;
    }

    public boolean handleFault(SOAPMessageContext context) {

        System.out.println("#####Fault soap message#####");
        logSoapMessage(context);

        return true;
    }

    public void close(MessageContext context) {

    }

    public void logSoapMessage(SOAPMessageContext context) {

        try {
            SOAPMessage msg = context.getMessage();

            ByteArrayOutputStream bas = new ByteArrayOutputStream();
            msg.writeTo(bas);
            System.out.println(bas);
        }
    }
}
```

```

    }
    catch (Exception e) {
        System.out.println("Error while writing SOAP message to debug log " + e);
    }
}

public Set<QName> getHeaders() {
    return null;
}

private void addAuthentication(SOAPHeader header) {
    try {

        SOAPElement security =
            header.addChildElement("Security", "wsse", "http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd");

        SOAPElement usernameToken =
            security.addChildElement("UsernameToken", "wsse",
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd");

        SOAPElement username =
            usernameToken.addChildElement("Username", "wsse");
        username.addTextNode("****");

        SOAPElement password =
            usernameToken.addChildElement("Password", "wsse");
        password.setAttribute("Type",
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText");

        password.addTextNode("****");

    } catch (Exception e) {
        e.printStackTrace();
    }
}
}

```

**Related
Documentation**

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Accessing a Web Service on page 62](#)
- [Profiles Used by Service Now on page 56](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

Accessing a Web Service

Access to a Web Service (WS) or a OSS/J Trouble Ticket (TT) API requires authentication. An OSS/J Client has to use a user name and password of Junos Space server when making calls through the OSS/J TT API to create and modify tickets on the trouble ticket management system.

The procedure to access web service is as follows:

1. The OSS/J client adds the authentication details in the SOAP header of a WS request.
2. The client requests are intercepted by JAX-WS handlers at WS server for getting authenticated.
3. JAX-WS handler parse the SOAP header to get the authentication details.
4. The username and password are authenticated by making REST call to Junos Space. If the authentication is successful, the web service request is forwarded to JVT profile to invoke the appropriate internal rest call to Service Now API.
5. The SOAPFault exception is thrown if authentication fails.

The Web Service messages comply with the WS_SECURITY standard. A dedicated security header defines properties for user and password that must be added.

Soap Header Template

```
<soapenv:Header>

<wsse:Security soapenv:mustUnderstand="0"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd"><wsse:UsernameToken
wsse:Id="UsernameToken-14327075"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><wsse:Username>***</wsse:Username><wsse:Password
Type="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">***</wsse:Password></wsse:UsernameToken></wsse:Security>

</soapenv:Header>
```

Related Documentation

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Profiles Used by Service Now on page 56](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

Trouble Ticket APIs Supported by Service Now

The client provides operations (getting, creating, changing or canceling/closing tickets) to manage and retrieve trouble tickets from the trouble ticket management system.

The following list of APIs from JSR91 specification are implemented in Service Now.

- createTroubleTicketByValue
- tryCreateTroubleTicketsByValues
- getTroubleTicketByKey
- getTroubleTicketsByKeys
- setTroubleTicketByValue
- trySetTroubleTicketsByValues
- trySetTroubleTicketsByKeys
- tryCancelTroubleTicketsByKeys
- tryCloseTroubleTicketsByKeys
- cancelTroubleTicketByKey
- closeTroubleTicketByKey
- getTroubleTicketTypes
- getEventTypes
- getEventDescriptor
- getManagedEntityType
- getSupportedOptionalOperations

The following table describes the trouble ticket APIs.

Table 8: Trouble Ticket APIs Supported by Service Now

Troube Ticket API	Description
createTroubleTicketByValue	Creates a single trouble ticket
tryCreateTroubleTicketsByValues	Creates multiple trouble tickets
getTroubleTicketByKey	Obtains a single trouble ticket using the given key and returns only the requested attributes
getTroubleTicketsByKeys	Obtains multiple trouble tickets using the given keys and returns only the requested attributes
setTroubleTicketByValue	Updates a single trouble ticket using the given value
trySetTroubleTicketsByValues	Best effort update of multiple trouble ticket items by the given values

Table 8: Trouble Ticket APIs Supported by Service Now (*continued*)

Troube Ticket API	Description
trySetTroubleTicketsByKeys	Best effort update of multiple trouble ticket items by the given keys
tryCancelTroubleTicketsByKeys	Cancels multiple trouble tickets indicated by the given keys
tryCloseTroubleTicketsByKeys	Best effort closing of multiple trouble tickets indicated by the given keys
cancelTroubleTicketByKey	Cancels a trouble ticket indicated by the given key
closeTroubleTicketByKey	Closes a trouble ticket indicated by the given key

**Related
Documentation**

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Profiles Used by Service Now on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

Error Messages Displayed by OSS/J Client

The error descriptions and the supported APIs for the various error scenarios are given as follows:

Table 9: OSS/J Client Error Scenarios

OSSJ Error Description	Supported APIs
JNPRERROR-998: Username and/or password are/is not valid in Space. Please check your entries in Space and resubmit your request. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1020: Organization is not configured in Service Now. Please check your entries in Service Now and resubmit your request. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1005: Juniper system is unresponsive at this moment. Please try again later. If the problem persists, please contact Juniper Customer Support.	All APIs

Table 9: OSS/J Client Error Scenarios (*continued*)

OSSJ Error Description	Supported APIs
JNPRERROR-1014: There is already an active Trouble Ticket for the supplied serial number, product, platform and trouble description combination. Trouble Ticket Id: 2013-0617-1021. Please use this Trouble Ticket Id if you wish to provide any additional information or updates to this issue.	createTroubleTicketByValue createTroubleTicketByValue
JNPRERROR-1013: Trouble Ticket Id 2013-0617-1022 in Juniper System is already Closed or Cancelled and cannot be updated. Please request for a new ticket through appropriate messaging.	setTroubleTicketByValue trySetTroubleTicketsByValues trySetTroubleTicketsByKeys tryCancelTroubleTicketsByKeys tryCloseTroubleTicketsByKeys cancelTroubleTicketByKey closeTroubleTicketByKey
JNPRERROR-1012: Juniper System could not validate the support entitlement for the supplied device 0000233004A. Please contact Juniper Customer Support to verify the support eligibility of the device.	createTroubleTicketByValue tryCreateTroubleTicketsByValues
JNPRWARN-1002: Product details like series and platform could not be determined from the information supplied in the Trouble Ticket. So an admin trouble ticket is created in Juniper System and assigned to Juniper Customer Care who is soon going to contact you to obtain relevant details before the Trouble Ticket can be assigned to the right Technical Engineer to troubleshoot the problem.	createTroubleTicketByValue tryCreateTroubleTicketsByValues
JNPRERROR-1027: Cannot create Trouble Ticket as Trouble Description, Trouble Detection Time, Suspect Object Id is null or empty. Trouble Description, Trouble Detection Time and Suspect Object Id are mandatory parameters for creating a Trouble Ticket. Please provide a valid input and resubmit your request.	createTroubleTicketByValue tryCreateTroubleTicketsByValues
JNPRERROR-1000: An unexpected error has occurred in the Juniper Backend System. Please try again later. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1021: Base State of a Trouble Ticket can only be OPEN, ACTIVE or QUEUED while creating a Trouble Ticket. Please provide a valid Base State and resubmit your request.	createTroubleTicketByValue tryCreateTroubleTicketsByValues

Table 9: OSS/J Client Error Scenarios (*continued*)

OSSJ Error Description	Supported APIs
JNPRERROR-1018: Cannot create or update Trouble Ticket as Customer Trouble Number is greater than 40 characters. Please provide a valid Customer Trouble Number that Service Now understands to create or update a Trouble Ticket.	createTroubleTicketByValue tryCreateTroubleTicketsByValues setTroubleTicketByValue trySetTroubleTicketsByValues trySetTroubleTicketsByKeys
JNPRERROR-1023: Primary key of a Trouble Ticket should not be null or empty while fetching or updating a Trouble Ticket. Please provide a valid Trouble Ticket Primary Key and resubmit your request.	getTroubleTicketByKey getTroubleTicketsByKeys setTroubleTicketByValue trySetTroubleTicketsByValues trySetTroubleTicketsByKeys tryCancelTroubleTicketsByKeys tryCloseTroubleTicketsByKeys cancelTroubleTicketByKey closeTroubleTicketByKey
JNPRERROR-999: [method name] API is not supported in OSS/J implementation of Service Now.	APIs that are not supported by Service Now implementation of JSR91.

Related Documentation

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Profiles Used by Service Now on page 56](#)

Trouble Ticket Attributes Supported by Service Now

The following table lists the attributes supported by Service Now.

Table 10: Supported Trouble Ticket Attributes

Trouble Ticket Attribute	Description	Access Right Provided to an External System
troubleTicketKey	Unique key to identify a trouble ticket.	Read access
additionalTroubleInfoList	Describes the reported trouble. It is represented by a set of graphic strings.	Read/write/access
attachmentData	Contains filename and data. The size of the data can be 6 MB (maximum) per attachment Base64 encoded. Attachments can be updated/added through update/create trouble ticket. If file name is not displayed, it is derived from the data. It will be assumed the name of the file in the attachment data will be the name of the file. If the attachment data has no file name, the attachment data will be given an arbitrary file name as attachment_1 and so on.	Only upload access
closeOutNarr	Provides additional information regarding the trouble report closure.	Read/write access
relatedTroubleTicketKeyList	Provides a list of related TRs.	Read access
troubleDescription	Provides a summary of the PR.	Write access is provided only at the first attempt. For all subsequent updates, only read access is provided.
baseState	Indicates the state of a ticket/case.	Read/write access
baseStatus	Indicates the status of a ticket/case	Read/write access
troubleDetectionTime	Indicates when the trouble was detected.	Read/write access
cancelRequestedByCustomer	Indicates whether the customer has requested to cancel the case. Cancellation request is not permitted if the case is already cleared or closed. The case is closed when a cancellation request is granted.	Write access
closeOutVerification	Indicates whether the customer has verified the resolution, denied the resolution, or taken no action.	Write access
customerTroubleNum	Specifies the internal number assigned to the customer (example, the number that is assigned by a customer's trouble administration system). It allows the customer to access the TTR with this internal number.	Read/write access

Table 10: Supported Trouble Ticket Attributes (*continued*)

Trouble Ticket Attribute	Description	Access Right Provided to an External System
basePreferredPriority	Specifies the urgency of the resolution required by the customer. Its value can be undefined, minor, major, or serious.	Read/write access
SuspectObjectList	Provides the list of objects that may be the underlying cause of the trouble. This list should be used to pass the device serial number.	Read/write access

Related Documentation

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Events Supported by Service Now on page 68](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Profiles Used by Service Now on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

Trouble Ticket Events Supported by Service Now

You can track a trouble ticket or a trouble ticket item that is created, modified or deleted, by means of notifications. Service Now supports the WS-BaseNotification (a standard defined by OASIS) to receive events (notifications).

To receive events through a Web Service, you need to subscribe to the server-side web service. The server-side web service implements administration tasks to manage the subscription. The client-side service implements methods to receive events.

The JSR91 standard events implemented by Service Now are described as follows:

- **TroubleTicketCreateEvent**—The trouble ticket management system publishes this event when a trouble ticket is created. This event must be the first event published for a specific trouble ticket.

Supported attributes: The trouble ticket must contain all the attributes listed in table “[Trouble Ticket Attributes Supported by Service Now](#)” on page 66. The trouble ticket must contain a value for the trouble ticket key to identify the trouble ticket.

- **TroubleTicketAttributeValueChangeEvent**—The trouble ticket management system publishes this event when the value of a trouble ticket attribute is modified. This includes update, closure or cancellation of a trouble ticket as well as changes during the execution of a trouble ticket.

Supported attributes: This event includes all the attributes listed in [“Trouble Ticket Attributes Supported by Service Now” on page 66](#). This event is published when a trouble ticket item is associated to or disassociated from a trouble ticket and also when the baseState or the baseStatus attributes are modified. This event must contain a value for the troubleTicketValue attribute and the value must contains all new values of the modified attributes. Attributes that are not changed are not populated.

- **TroubleTicketStatusChangeEvent**—The trouble ticket management system publishes this event when the status of a trouble ticket is changed. When the status of the trouble ticket changes, both TroubleTicketAttributeValueChangeEvent and TroubleTicketStatusChangeEvent are published. This event is published when the values of the baseState and the baseStatus attributes are modified.

Supported attributes: The event contains the mandatory attribute troubleTicketKey that holds the key value of the affected trouble ticket, and the baseState and the baseStatus attributes that hold the state value of the new trouble ticket.

- **TroubleTicketCloseOutEvent**—The trouble ticket management system publishes this event when a trouble ticket is closed.

Supported attributes: This event extends the event type TroubleTicketStatusChangeEvent and thus contains the same attributes used in TroubleTicketStatusChangeEvent, and is used in the same method as TroubleTicketStatusChangeEvent. The mandatory attributes baseState and baseStatus contain the new values. The other attribute value of a trouble ticket contains the history information of the closed trouble ticket. This includes the change of state due to a closed or an updated operation as well as changes during the execution of a trouble ticket implementation.

Related Documentation

- [Service Now Overview on page 34](#)
- [Trouble Ticket APIs Overview on page 55](#)
- [Trouble Ticket APIs Supported by Service Now on page 63](#)
- [Trouble Ticket Attributes Supported by Service Now on page 66](#)
- [Setting up Java Based Web Service Client on page 56](#)
- [Profiles Used by Service Now on page 56](#)
- [Accessing a Web Service on page 62](#)
- [Error Messages Displayed by OSS/J Client on page 64](#)

CHAPTER 6

Administration

- [Administration Overview on page 71](#)
- [Organizations on page 72](#)
- [Device Groups on page 83](#)
- [Service Now Devices on page 86](#)
- [Event Profiles and AI-Scripts on page 108](#)
- [Global Settings on page 123](#)
- [Auto Submit Policy on page 134](#)
- [Address Group on page 144](#)
- [E-mail Templates on page 151](#)

Administration Overview

You can use Service Now to monitor and manage a device with the help of AI-Scripts that are installed on the device. When AI-Scripts are installed on a device, the device is considered AI-Scripts-enabled and can automatically detect and report incidents and informational JMBs to Service Now.

You can also add devices that are part of the Junos Space platform to Service Now and group them under organizations. An organization is defined by a unique site ID that acts as a customer record in Juniper Networks CRM systems. After creating an organization, you can test its connectivity with JSS and even run it in test mode. Juniper Support Systems (JSS) provides support for the incidents and iJMBs that you submit. This support depends on your service contract level, such as J-Care Efficiency, Continuity, or Agility.

If you are a Juniper Networks partner or a direct customer with multiple distinct networks, you can use multiple Service Now organizations to keep customers or networks separate. Service Now organizations are defined by the site ID (used when opening support cases) under devices and users.

By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes and control a user's access to devices. Device groups also help you automatically install AI-Scripts on several devices at the same time.

Some administration tasks, such as adding connected members and viewing messages assigned to them, are enabled only when Service Now mode is activated. For more information about Service Now modes, see [“Service Now Modes” on page 42](#).

The Administration workspace enables you to perform the following tasks:

- Add devices to Service Now from the Junos Space platform.
- Add or delete an event profile or a script bundle.
- Add and delete devices and device groups.
- Install or remove AI-Scripts on devices.
- Associate devices with device groups.
- Add, modify, or delete organizations.
- Add connected members and view messages assigned to them (enabled if you are a Juniper Networks partner and running Service Now in the partner proxy mode).
- Run organizations in test mode and test organization connectivity to JSS.
- Export device data in CSV and Excel formats.
- Export inventory information in CSV format.
- Configure the global settings (SNMP server and proxy server settings).

**Related
Documentation**

- [Service Now Overview on page 34](#)
- [Service Now Modes on page 42](#)
- [Organizations Overview on page 73](#)
- [Device Groups Overview on page 83](#)
- [Service Now Devices Overview on page 86](#)
- [Event Profiles Overview on page 109](#)
- [AI-Scripts Overview on page 21](#)
- [Auto Submit Policy Overview on page 135](#)
- [Configuring Global Settings on page 123](#)

Organizations

- [Organizations Overview on page 73](#)
- [Adding an Organization on page 75](#)
- [Adding a Connected Member on page 77](#)
- [Modifying Organization Parameters on page 79](#)
- [Deleting an Organization on page 79](#)
- [Test the Connection to JSS on page 80](#)
- [Viewing Messages Assigned to a Connected Member on page 81](#)

- [Running an Organization in Test Mode on page 82](#)
- [Updating Core File Upload Configuration on page 82](#)

Organizations Overview

An organization in Service Now represents a unique Clarify site ID in Juniper Support Systems (JSS). JSS uses Clarify Site IDs to identify customers when providing technical support. You can manage multiple sites (each with its own Clarify site ID) using multiple organizations defined in Service Now with just one Service Now installation. This is done by dividing the network into multiple logical customer sites. To communicate with JSS, a Service Now organization requires a site ID, login name, and password. The login name must be a contact associated with the site ID.

Device groups are used to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Using device groups, you can control the access that users have over devices. See [“Device Groups Overview” on page 83](#).

For more information about creating device groups, see [“Creating a Device Group” on page 83](#).

While you configure organizations to run Service Now in a preproduction environment, you can avoid the processing of production incident cases by running an organization in test mode. In this mode, the synopsis of the incident is appended with [Test] so that JSS recognizes it as a test case and does not process it.

Service Now organizations are displayed in the Organizations page in the tabular format as shown in [Figure 4 on page 73](#).

Figure 4: Manage Organizations Page

Name	Site ID	Submit Cases As	User Name	Connection Status
EndCustomer1	---	---	ec@example.com	None Attempted
JCare-Plus	1-4XUVRM	Real Cases	test@example.com	Success
New_org	CJ18841	Real Cases	pvsuser@example.com	Success

[Table 11 on page 73](#) describes the fields displayed in the tabular view of the Manage Organizations page and in the **Organizations Details** dialog box.

Table 11: Organization Column Descriptions

Column Name	Description
Name	Name of the organization.

Table 11: Organization Column Descriptions (*continued*)

Column Name	Description
Site ID	Identifier for the Customer Site in the JSS Clarify system.
Submit Cases As	Specifies if the cases from a production environment should be submitted to JSS as a real case or a test case. The synopsis of a test case sent to JSS is appended with [Test Mode]. When Service Now is in offline mode, this column is empty.
User Name	User name to identify the user for communications with the JSS while creating cases or checking for updates. You do not need to enter a user name or password if Service Now is in the offline mode.
Connection Status	Status of the connection between the organizations and JSS.
JMB Filter Level	Filter for device configuration information in a JMB to be shared with JSS. (Only visible in the Detail Summary dialog box, which opens when you double-click the organization)

In the Organizations menu, you can:

- Add an organization
- Add a connected member
- Modify organization parameters
- Test an organization
- Test connectivity to JSS
- Delete an organization
- Associate address group
- Update core-file upload configuration



NOTE: This action is available only for connected member in partner proxy mode.

Related Documentation

- [Adding an Organization on page 75](#)
- [Adding a Connected Member on page 77](#)
- [Modifying Organization Parameters on page 79](#)
- [Deleting an Organization on page 79](#)
- [Test the Connection to JSS on page 80](#)

- [Viewing Messages Assigned to a Connected Member on page 81](#)
- [Running an Organization in Test Mode on page 82](#)
- [Associating Devices with an Address Group From an Organization ILP on page 148](#)
- [Updating Core File Upload Configuration on page 82](#)

Adding an Organization

An organization in Service Now represents a unique Clarify site ID in Juniper Support Systems (JSS). Clarify Site IDs identify customers when JSS provides technical support. You can use multiple organizations defined in Service Now to manage multiple sites (each with its own Clarify site ID) with only one Service Now installation. This is done by dividing the network into multiple logical customer sites. To communicate with JSS, a Service Now organization requires a site ID, login name, and password. While creating an organization, you can specify the device configuration information in JMBs that you want to share with JSS.

To add a Service Now organization in partner proxy mode:

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

The **Add Organization** dialog box appears.

Figure 5: Add Organization Dialog Box

2. Enter the organization parameters in the provided fields.
For a detailed description of these fields, see [Table 12 on page 76](#).



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

3. Click **Submit**.

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

To add a Service Now organization in end-customer mode:

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

The Add Organization dialog box appears.

2. Enter the organization parameters in the provided fields.
For a detailed description of these fields, see [Table 12 on page 76](#).
3. Click **Submit**.

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



NOTE: In end-customer mode, you can add only one organization.

[Table 12 on page 76](#) defines the **Add Organization** dialog box fields.

Table 12: Organization Credentials Page Field Descriptions

Name	Description	Privileges	Range/Length	Default
Name	Name of the organization	Service Now administrator privileges	64 characters	
Submit cases as	Specifies if the cases from this organization is to be submitted as real case or test case. The synopsis of a test case sent to JSS is appended with [Test Mode].	Service Now administrator privileges	The values are: <ul style="list-style-type: none"> • Real cases • Test cases 	Real Cases
User Name	Name used to identify the user for communications with the JSS while creating cases, and checking for updates to existing cases You do not need to enter a user name or password if Service Now is in the offline mode.	Service Now administrator privileges	32 characters	
User Password	Password for the username required for communicating with JSS. You do not need to enter a user name or password if Service Now is in the offline mode.	Service Now administrator privileges	32 characters	

Table 12: Organization Credentials Page Field Descriptions (*continued*)

Name	Description	Privileges	Range/Length	Default
Get Sites (button)	<p>Identifier for the Customer Site in the JSS Clarify system.</p> <p>Click Get Sites and select a Site ID from the Site ID list that is generated when you enter the username and password.</p> <p>NOTE: This option is not available when you add an organization in the end-customer mode.</p>	Service Now administrator privileges	80 characters	
JMB Filter Level	<p>The device configuration information in JMBs to be shared with JSS:</p> <ul style="list-style-type: none"> Do not send—does not send any device configuration information Send all information except configuration—Sends all device information except the configuration information Send all information with IP Addresses overwritten—Sends all device information with overwritten IP addresses Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information 	Service Now administrator privileges	—	Send all information with IP addresses overwritten

- Related Documentation**
- [Organizations Overview on page 73](#)
 - [Running an Organization in Test Mode on page 82](#)

Adding a Connected Member

After Service Now is configured to run in partner-proxy mode, multiple customers (connected member) can be added and managed over a secure HTTPS connection. To communicate with the customer, the Service Now application at the customer location should be activated. For information about end-customer mode, see “[Service Now Modes](#)” on page 42.



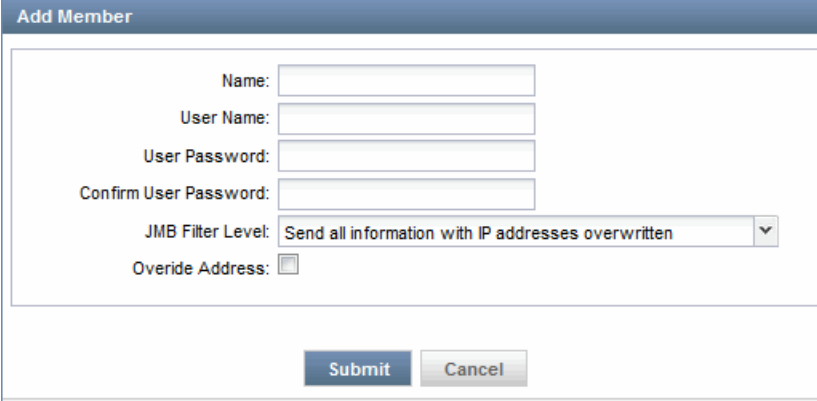
NOTE: A connected member can be added only after a valid organization is created.

To add a connected member to Service Now configured in the partner proxy mode:

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

The **Add Member** dialog box appears as shown in [Figure 6 on page 78](#).

Figure 6: Add Member Dialog Box



2. Enter a name for the connected member.
The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-). The maximum number of characters allowed is 64.
3. Enter a username for the connected member. The customer should use this username when submitting cases to the Juniper Networks partner.
The username must be in the format user@example.com.
4. Enter a password for the username.
5. Enter the same password again to confirm.
6. Select one of the following values to specify the device configuration information in a JMB that can be shared with the Juniper Networks partner and JSS:
 - Do not send—does not send any device configuration information.
 - Send all information except configuration—Sends all device information except the configuration.
 - Send all information with IP Addresses overwritten—Sends all the device information; however, the IP addresses associated with the device are overwritten.
 - Send all information—Sends all the device information.
 - Only send list of features used—Sends only the device configuration information.
7. If you select the **Override Address** check box for auto submit policy, a customer Return Materials Authorization (RMA) Incident is submitted to JSS with the address associated to the device by Partner. If you do not select the **Override Address** check box, the

address configured by the end customer is associated with a device when submitting a case.

8. Click **Submit**.

The connected member is created and displayed on the Organizations page.

**Related
Documentation**

- [Adding an Organization on page 75](#)
- [Organizations Overview on page 73](#)

Modifying Organization Parameters

Using Service Now, you can modify the parameters of an organization.



NOTE: You cannot edit the name of the connected member and the organization associated with it. For more information about connected members, see [“Service Now Modes” on page 42](#).

To modify the parameters of an organization:

1. From the Service Now navigation tree,, select **Administration > Organizations**.
The Organizations page appears.
2. Select the organization whose parameters you want to modify.
3. Click **Modify Organization** from either the **Actions** list or the right-click menu.
The Modify Organization appears.
4. Make changes to the organization parameters.
5. Click **Submit**.

The changes are saved in the Service Now database. To view these changes, view the details of the organization in the Organizations page.

**Related
Documentation**

- [Organizations Overview on page 73](#)
- [Deleting an Organization on page 79](#)
- [Running an Organization in Test Mode on page 82](#)

Deleting an Organization

As a Service Now administrator, you can use the Service Now Organizations page to delete organizations.



NOTE: You cannot delete an organization without first deleting its associated connected members.

To delete an organization:

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

The Organizations page appears.

2. Select the organization that you want to delete.

3. Click **Delete Organization** from the **Actions** list or the right-click menu.

The **Delete Organizations** dialog box appears asking you to confirm the deletion.

4. Click **Delete**.

The selected organization is deleted from the Service Now database and no longer appears in the Organizations page.



NOTE: When you delete an organization, you also automatically delete its associated device groups.

Related Documentation

- [Organizations Overview on page 73](#)
- [Adding an Organization on page 75](#)
- [Running an Organization in Test Mode on page 82](#)

Test the Connection to JSS

From the Organizations page, you can test the connection of every organization with Juniper Support Systems (JSS).

To test an organization's connectivity with JSS:

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

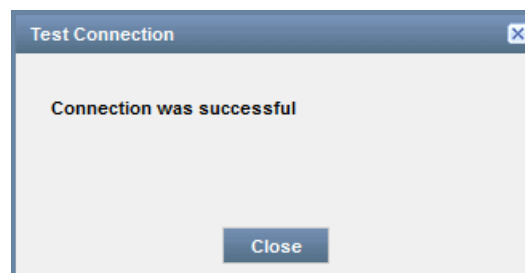
The Organizations page appears.

2. Select the organization whose connection to JSS you want to test.

3. Click **Check Status** from either the **Actions** list or the right-click menu.

The **Test Connection** dialog box displays the result of the test connection to JSS, as a success or a failure.

Figure 7: Test Connection Dialog Box



In case of a failure, a description appears stating the reason for the connection failure.

4. Click **Close** to return to the Organizations page.



NOTE: You cannot check the connectivity status when Service Now works in the offline mode.

Related Documentation

- [Organizations Overview on page 73](#)
- [Adding an Organization on page 75](#)
- [Deleting an Organization on page 79](#)
- [Running an Organization in Test Mode on page 82](#)

Viewing Messages Assigned to a Connected Member

Using Service Now, you can view the list of messages that are assigned to a customer (connected member) . This action is available only when Service Now operates in the partner-proxy mode and when you select a connected member in the Organizations page.

To view the messages assigned to a connected member:

1. From the Service Now navigation tree, select **Administration > Organizations**.
The Organizations page displays the list of organizations and connected members.
2. Select the connected member whose list of assigned messages you want to view.
3. Right-click your selection and select **View Messages** from either the **Actions** list or the right-click menu.

As shown in [Figure 8 on page 81](#), the Messages assigned to Connected Member page displays the list of messages assigned to the selected connected member.

Figure 8: Messages Assigned to Connected Member Page

Administration > Organizations > View Messages		
Messages assigned to Connected Member		
Return to Organization		
Title	Status	Sent
Junos Space Service Now Deployment	Staged for Connected Member	

4. To view the details of the messages, click the title of the message.

The **Message Details** dialog box displays information such as the organization that the message is sent to, site ID, title, issue date, summary, instructions, keywords, relevance, owner, and the users that the message was flagged to.

5. Click **OK** to return to the Organizations page.

Related Documentation

- [Assigning a Message to a Connected Member on page 178](#)
- [Messages Overview on page 175](#)

- [Adding a Connected Member on page 77](#)

Running an Organization in Test Mode

While configuring an organization, you can enable test mode so that you can submit cases as test cases and avoid the processing of production incident cases. In this mode, the synopsis of the incident that is submitted to JSS is appended with [Test].

To run an organization in test mode:

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

The Organizations page appears.

2. Select the organization that you want to place in test mode, and select **Modify Organization** from either the **Actions** list or the right-click menu.

The Modify Connected Member dialog box displays the parameters of the selected organization.

3. Select **Test Cases** from the **Submit Cases as** list.
4. Click **Submit**.

This action ensures that incidents that are submitted to JSS are considered as test cases.

Related Documentation

- [Organizations Overview on page 73](#)
- [Modifying Organization Parameters on page 79](#)

Updating Core File Upload Configuration

You can update the core file configuration for a connected member in partner proxy mode. This feature is enabled only for a connected member. If this feature is not enabled, you can use the default setting to upload core files. For more details, see [“Uploading Core Files Generated for Events” on page 133](#).

To change the core file configuration for a connected member:

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

The Organizations page is displayed.

2. Select the organization whose configuration you want to change.

3. Click **Update Core File Upload Configuration** from either the **Actions** list or the right-click menu.

The Modify Core File Upload Configuration for Connected Member dialog box appears.

4. Fill in the required parameters in the displayed fields, and click **Submit**.

The configuration is successfully changed.

- Related Documentation**
- [Organizations Overview on page 73](#)
 - [Administration Overview on page 71](#)
 - [Uploading Core Files Generated for Events on page 133](#)

Device Groups

- [Device Groups Overview on page 83](#)
- [Creating a Device Group on page 83](#)
- [Modifying Device Groups on page 85](#)
- [Deleting Device Groups on page 85](#)

Device Groups Overview

You can use Service Now to group network elements and manage multiple devices in a single entity called a device group. You use device groups to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. You can associate one or more devices with every device group.

Only users with Service Now administrator privileges can configure device groups.

From the Device Groups page in Service Now, you can perform the following tasks:

- Create a device group and add devices to it
- Modify device groups
- Delete device groups
- Associate address groups
- Set default device group

- Related Documentation**
- [Creating a Device Group on page 83](#)
 - [Modifying Device Groups on page 85](#)
 - [Deleting Device Groups on page 85](#)
 - [Associating Devices with an Address Group from a Device Group ILP on page 149](#)

Creating a Device Group

You use device groups to group devices within an organization. Only users with Service Now administrator privileges can create device groups and add devices to them. All the new devices are associated to a device group by default.

Creating a new Service Now Organization in Standard mode:

- When a new organization is created, Service Now automatically creates a device group and associates it with the organization.

- You can edit and delete device groups that Service Now creates for the organization.

Creating a New Service Now Organization in Partner-Proxy Mode:

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

Figure 9: Create Device Group Page

2. Enter a name for the device group within the **Name** field.
The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-). The maximum number of characters allowed is 64.
3. In the **Organizations** list, select an organization for this device group.
If you want to add a new organization, click **New Organization**. See [“Adding an Organization” on page 75](#).

4. Select the devices that you want to add to this device group.
5. Click **Add**.

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

- Related Documentation**
- [Device Groups Overview on page 83](#)
 - [Modifying Device Groups on page 85](#)

Modifying Device Groups

To modify a device group:

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

The Device Group page lists the existing device groups.

2. Select the device group whose parameters you want to modify, and select **Modify Device Group** from either the **Actions** list or the right-click menu.

The Edit Device Group page appears and displays the parameters of the selected device group.

3. Modify the fields as necessary.

For Service Now running in partner-proxy mode, you can set any device group as the default while modifying the device group. This is done by selecting the **Set as Default** check box. However, if the user does not select the **Set as Default** check box, an error message appears stating **Please set other device group as the default device group before unselecting this device group as the default**.

Use the **Device Groups** navigation drawer on the right-hand side of the screen to add or delete devices from the selected device group.

4. Click **Finish**.

The changes are submitted and new values are replaced in the Service Now database. The Device Group page appears.

- Related Documentation**
- [Device Groups Overview on page 83](#)
 - [Deleting Device Groups on page 85](#)
 - [Creating a Device Group on page 83](#)

Deleting Device Groups

If you have Service Now administrator privileges, you can delete device groups.

To delete a device group:

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

The Device Group page lists the existing device groups.

2. Select the device group that you want to delete, and select **Delete Device Group** from either the **Actions** list or the right-click menu.

The **Delete Device Group** dialog box prompts you to confirm the deletion.

3. Click **Delete**.

The selected device group is deleted from the Service Now database and no longer appears on the Device Group page.

**Related
Documentation**

- [Device Groups Overview on page 83](#)
- [Modifying Device Groups on page 85](#)

Service Now Devices

- [Service Now Devices Overview on page 86](#)
- [Adding Devices from the Platform on page 90](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Uninstalling Event Profiles from Devices on page 94](#)
- [Exporting Device Data in CSV and Excel Format on page 94](#)
- [Exporting Inventory Information in CSV Format on page 95](#)
- [Viewing Exposure on page 96](#)
- [Generating On-Demand Incidents on page 96](#)
- [Collecting RSI and System Log Files on page 100](#)
- [Requesting RMA Incidents on page 103](#)
- [Deleting a Device on page 105](#)
- [Associating Devices with a Device Group on page 105](#)
- [Modifying Auto Submit Policy on page 106](#)
- [Viewing Incidents on page 107](#)
- [Verifying Connection between Devices and FTP Server on page 108](#)

Service Now Devices Overview

You can use Service Now to group network elements and manage multiple devices in a single entity called a device group. Service Now lists the devices that are already a part of the Junos Space platform and that you can import into Service Now. You can view only those devices for which you have permission (based on the role-based access control [RBAC] policy) and other Service Now-defined objects. These devices periodically send device information (device snapshots) to Service Now for monitoring purposes. Service Now detects the devices that have not sent device snapshots for more than 10 days and identifies them on the Service Now GUI.

Service Now generates iJMBs automatically for all devices associated with a device group. When the devices stop sending iJMBs, Service Now uses the directive file (.directive) to

generate the iJMBs. The directive file contains commands required to generate iJMBs. For information about iJMBs, see [Device Snapshots Overview](#).

After you add devices and create device groups, you can perform various operations on them, such as installing and removing AI-Scripts individually on every device or on all the devices in a device group simultaneously. You can also delete devices from the Service Now database.

Service Now devices are displayed on the Service Now Devices page. They are arranged according to organization, device group, hostname, serial number, platform, version, state (added or removed state of end-customer devices only), and script bundle. Table 1 describes the columns on the Service Now Devices page and in the Device Detail dialog box.

Field Name	Description
Organization	Name of the organization to which this device belongs
Connected Member	Name of the connectedmember
Device Group	Name of the device group to which this device belongs
HostName	Unique name by which the device is known on a network
IP Address	IP address of the device
Serial Number	Serial number of the device
Product	Type of the device. For example, MX960 and EX4200.
Version	Version of the Junos OS that is running on the device
State	By default, this field is hidden. It is displayed only for end-customer devices in a Service Now device operating in partner proxy mode. The values for this field are Added and Removed.
Script Bundle	Name and version of the script bundle installed on the device
Event Profile	Name and version of the event profile installed on the device
Ship-to Address	Address to which the device or device parts should be shipped
Location	Location of the device
Domain	Domain to which the device is assigned
Policy	All autosubmit policies associated with this device for submitting incidents to a Service Now partner or Juniper Support Systems. Each policy name is separated by a comma.
Platform	Model of the device.

Field Name	Description
Routing Engine	Type of Routing Engine. The values are: <ul style="list-style-type: none"> • Single Routing Engine • Dual Routing Engines
Event Profile Installation Status	Installation status of an event profile on the device. The values are: <ul style="list-style-type: none"> • Success • Failed • Master RE Failed • Backup RE Failed • Successfully installed in Master RE. Backup RE is inactive.
Connection Status	Status of connection between the device and Service Now
Alerts	Status of iJMB received from the device
Support Contract Information	Table to display information about the support contract for the device. The fields included in the table are—contract number, status, SKU, SKU type, as well as start and end dates of the contract. <p>To get on-demand updates about your Service Now contract, click the Refresh button on the Device Details page.</p>

Only users with Service Now administrator privileges can configure device groups.

The  icon is displayed on the Service Now Devices page under the following conditions:

- When there is a mismatch between the versions of AI-Scripts installed on a device and AI-Scripts bundle present on Service Now or when Service Now does not have an AI-Scripts bundle uploaded, but the device has AI-Scripts installed on it.

If you place the cursor on the icon, the tool tip displays the following message:

There is a mismatch of the AI-Scripts installed on routing engine, on device.

For example:

There is a mismatch of AI-Scripts installed on 'fpc0' of device ex-4200-sn1

For a device with dual Routing Engines, routing engine indicates the Routing Engine on which the version of AI-Scripts installed is different from the AI-Scripts bundle present on Service Now. If the version of AI-Scripts installed on both the Routing Engines is different from the AI-Scripts bundle present on Service Now, the following message is displayed:

There is a mismatch of the AI-Scripts installed on routing engine 1, routing engine 2, on device.

For example:

There is a mismatch of AI-Scripts installed on 're0', 're1' of device mx-104-sn.

There can be a mismatch between the versions of AI-Scripts installed on a device and Service Now for the following reasons:

- Service Now is unaware of the version installed on a device—for example, when you add a device to Service Now that already has AI-Scripts installed on it.
- If after installing AI-Scripts on a device by using Service Now, AI-Scripts are manually deleted from the device.
- When one or more JMB files, attachments, and log files are not deleted from a device after copying the files from the device to Service Now.

If you place the cursor on the icon, the tool tip displays the following message:

one or more files (JMB/Attachments/Logs) could not be deleted from the device.

These files contain the `_ais_` string in their name and must be deleted manually from the `/var/tmp` directory of the device.

From the Service Now Devices page, you can perform the following tasks:

- Add devices from the platform.
- Install event profiles on the devices.
- Remove event profiles from the devices.
- Export device data in CSV and Excel formats.
- Export inventory information in CSV format.
- Modify the autosubmit policy.
- Delete devices.
- View information about the device that risk the chance of exposure to known issues.
- Associate devices with a device group.
- Associate devices with an address group.
- View the incidents for the devices supported by Service Now.
- Generate on-demand incidents.
- Request RMA incidents.
- Verify the connection between the devices and FTP server.

**Related
Documentation**

- [Adding Devices from the Platform on page 90](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Uninstalling Event Profiles from Devices on page 94](#)
- [Exporting Device Data in CSV and Excel Format on page 94](#)
- [Exporting Inventory Information in CSV Format on page 95](#)
- [Viewing Exposure on page 96](#)
- [Modifying Device Groups on page 85](#)
- [Deleting a Device on page 105](#)
- [Associating Devices with a Device Group on page 105](#)

- [Associating Devices with an Address Group From a Service Now Devices ILP on page 150](#)
- [Viewing Incidents on page 107](#)
- [Generating On-Demand Incidents on page 96](#)
- [Verifying Connection between Devices and FTP Server on page 108](#)
- [Requesting RMA Incidents on page 103](#)

Adding Devices from the Platform

You can add devices that are a part of the Junos Space Network Management Platform to the Service Now application. While you add these devices, you can also assign them to a device group and also install AI-Scripts on them.



NOTE: Devices that are discovered and added to the Junos Space platform are automatically added to the Service Now application. However, if Service Now is in demo mode, only the first five devices are added.

To add devices from the Junos Space platform to Service Now:

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

The Select Devices to Add to Service Now and Click Submit page displays the devices that have not been added to Service Now.

Figure 10: Select Devices to Add to Service Now and Click Submit Page

Select Devices to Add to Service Now and Click Submit				
<input type="checkbox"/> Host Name	IP Address	Serial Number	Product	Version
<input checked="" type="checkbox"/> g26-p2	192.0.2.1	mmmmmmmm	ACX2000	12.3-20130929_acx_x51_s1.0

2. Select the devices that you want to add.
3. Click **Submit**.

The Add Service Now Device(s) page appears.

4. Click **Apply profiles to added device(s) (manually)** to go to the Install Event Profile page. For more information on installing profiles, see [“Installing an Event Profile on Devices Using Service Now”](#) on page 91.

The devices are added to Service Now and displayed on the Service Now Devices page. The device **Status** column displays **Imported**.

- Related Documentation**
- [Service Now Devices Overview on page 86](#)
 - [Installing an Event Profile on Devices Using Service Now on page 91](#)
 - [Modifying Auto Submit Policy on page 106](#)

Installing an Event Profile on Devices Using Service Now


An event profile is a set of event scripts that are selected from an AI-Scripts bundle. When you install an event profile on Juniper Networks devices, the event scripts provide the information needed to automatically detect and report problem (incident) and information events, thus ensuring maximum network uptime.

Service Now uses the Device Management Interface (DMI) to install and remove AI-Scripts on devices. DMI is an extension to the NETCONF network management protocol.

When you install event profiles on individual systems (chassis) with dual Routing Engines, Service Now installs the event profiles on both primary and backup Routing Engines.



NOTE: While operating in partner-proxy mode, you cannot install event profiles on a connected member's device.

The  icon appears on the device Inventory Landing Page if the versions of the AI-Scripts installed on a Routing Engine and Service Now are different. For a dual Routing Engine, the icon also indicates that the version of the AI-Scripts installed on the primary and backup Routing Engines are different. If you place the cursor on the icon, the tool tip displays the following message:

There is a mismatch of the AI-Scripts installed on *routing engine* on *device*.

To install an event profile on devices:

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

The Service Now Devices page appears.

2. Select the device on which you want to install the event profile. If you have selected one or more devices for installing the event profile, the Install Event Profile action is active even if the devices are not associated with an organization or Device Group.
3. Click **Install Event Profile** from either the **Actions** list or the right-click menu.

The Install Event Profile dialog box appears as shown in [Figure 11 on page 92](#).

Figure 11: Install Event Profile Dialog Box

4. Select the appropriate Device Group from the **Add to Device Group** field.
A user can choose a device group before installing event profile. All the selected devices get associated to the selected device group.
5. Select an event profile from the **Use Profile** field.
6. (Optional) If you do not want to save a copy of the event profile after it is installed on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.
7. (Optional) If you want to remove the script bundle from the device after it is installed, select the **Remove Script Bundle files after successful install** check box.



NOTE: The two optional options are not available during the installation of AI scripts on the , QFX3000-M, QFX3000-G and EX with Dual RE devices.

8. (Optional) If you want to schedule a time for installation, select the **Schedule at a later time** check box, and specify the **Date and time** for the installation.
The installation process begins automatically at the time you specify.
9. Click **Submit**.
10. (Optional) If you want to add devices on which you want to install the selected event profile, select the **Install Event Profiles on new Devices** check box, and select the devices.
11. Click **Finish**.

The **Save Event Profile** dialog box appears.

12. Click one of the following links based on the required results.

Link	Result
Apply this profile to original set of devices	The Potential Exposure to Known Issues page displays information about the selected set of devices. A bang (!) icon is placed next to devices, associated with the event profile, that risk the chance of exposure.

Figure 12: Potential Exposure to Known Issues Page

Device Name	Serial Number	Product	Version	Exposure
ex-2200-sn3	CW0210403356	EX2200-24T-4G	12.2R3.5	Click

- a. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
- b. (Optional) To view a device's exposure to known issues, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated with the respective device.
Click **Return to Potential Exposure** to continue.
- c. Click **Continue**.
A confirmation pop-up box procedures the final procedure of devices on which the selected event profile must be installed.
You can remove devices from the procedure by clearing the check boxes of the devices you want to delete.
- d. Click **Install**.
The selected event profile is installed on the devices with which it is associated, and the Service Now Devices page appears.
To view the status of the event profile installation task, click the job ID link and the Jobs page displays the status of the job. Double-click the job to view information about each step of the installation.

Apply this profile to devices manually

You can select devices manually on which you want to install the event profile. Select the devices and click **OK**. The **Job Information** dialog box displays the job ID. To view the status of the event profile installation task, click the job ID link and the Jobs page displays the status of the job. Double-click the job to view information about each step of the installation.

Click **OK** to return to the Event Profiles page.

Link	Result
Return to the Profiles Page	The event profile installation task is canceled, and the Event Profiles page appears.

Related Documentation

- [Event Profiles Overview on page 109](#)
- [AI-Scripts Overview on page 21](#)
- [Manually Installing AI-Scripts on Devices on page 29](#)
- [Adding a Script Bundle to Service Now on page 121](#)
- [Viewing Exposure on page 96](#)

Uninstalling Event Profiles from Devices

You can use Service Now to uninstall event profiles from devices. You cannot uninstall event profiles from devices that do not have proper login credentials. Service Now uses Device Management Interface (DMI) to install and remove event profiles on devices. DMI is an extension to the NETCONF network management protocol.



NOTE: While operating in partner-proxy mode, you cannot uninstall event profiles from a connected member's device.

To uninstall event profiles from devices:

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

The Service Now Devices page appears.

2. Select the devices from which you want to uninstall event profiles, and select **Uninstall Event Profile** from either the **Actions** list or the right-click menu.

A message appears asking you to confirm the deletion.

3. Click **Submit**.

Event profiles are uninstalled from the selected devices.

To view the status of this task, click the job ID link. The Jobs page displays the status of the job. Double-click the job to view each step of the uninstallation.

Related Documentation

- [AI-Scripts Overview on page 21](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)

Exporting Device Data in CSV and Excel Format

You can export Service Now device data to CSV and Excel file formats. A CSV file is a plaintext file that stores each data record separated by a comma. The XML file contains the hardware components installed in the selected device.

To export the device data in CSV and Excel format:

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

The Service Now Devices page appears.

2. Select the device whose data you want to export, and select **Export Devices** from either the **Actions** list or the right-click menu.

The **Export Devices** dialog box is displayed.

3. Export the device information:

- click the **Export Devices in CSV Format** to export the device data in CSV format.
- click the **Export Devices in Excel Format** to export the device data in Excel format.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Deleting a Device on page 105](#)
- [Modifying Auto Submit Policy on page 106](#)

Exporting Inventory Information in CSV Format

You can export a customer's device inventory information to CSV and Excel file formats. A CSV file is a plain text file that stores each data record separated by a comma.

To export the inventory information:

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

The Service Now Devices page appears.

2. Select the device whose data you want to export.

3. Select **Export Inventory Information** either from the **Actions** list or the right-click menu.

The Export Inventory Information dialog box is displayed.

4. Export the inventory information:

- click the **Export Inventory Information in CSV format** link to export the inventory information to a CSV file.
- click the **Export Inventory Information in Excel format** link to export the inventory information to an Excel file.

The Export Inventory Job Status dialog box appears and shows the job status.

5. After the job is complete, click the **Download** link to either open or save the CSV or Excel file.

The following inventory information are listed: device name, item, model number, part number, serial number, location, ship to address, EOL status, EOL replacement part, EOL date, and description.



NOTE: The device inventory of end-customer devices takes one day to be reflected in the mode.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Deleting a Device on page 105](#)
- [Modifying Auto Submit Policy on page 106](#)
- [Viewing Exposure on page 96](#)

Viewing Exposure

The Service Now Devices page displays a bang (!) icon next to a organization with devices that are susceptible to known issues.

Using Service Now, you can view details of these exposed devices. The details include the device name, Junos OS version, script bundle, and associated information messages as well as a link to the problem report (PR) and a description of the problem.



NOTE: This feature is not available if Service Now is in offline mode.

To view information about the devices that are susceptible to known issues:

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

The Service Now Devices page appears.

2. Select the device that is susceptible (with the (!) icon) and click **View Exposure** from either the **Actions** list or the right-click menu.

The View Exposure page appears and displays the device name, product, version, PR, and PR synopsis.

3. Click **Return to Device View** to go back to the Service Now Devices page.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Adding Devices from the Platform on page 90](#)
- [Deleting a Device on page 105](#)
- [Modifying Auto Submit Policy on page 106](#)
- [Collecting RSI and System Log Files on page 100](#)

Generating On-Demand Incidents

Using Service Now, you can create Juniper Message Bundles (JMBs) for specific devices without having to wait for an event to trigger an incident. These JMBs are called on-demand incident JMBs. You can choose to generate on-demand JMBs using scripts

or remote commands run by Service Now. If you are using remote commands run by Service Now, the JMBs are constructed using the **directive.rc** file preloaded in Service Now. When you submit an on-demand incident to the device, Service Now calls an on-demand incident profile, which triggers an event and generates the incident. These profiles are predefined by Juniper Networks and contain information such as the type of incident and the remote procedure calls (RPCs) used to trigger the incident.

Service Now automatically submits these JMBs to the Juniper Support Systems (JSS) for creating a case. To avoid submitting incidents automatically, clear the **Automatically Submit Cases** check box on the On-demand Incident dialog box.



NOTE:

- To create an on-demand incident, AI-Scripts Release 3.2 R1 or later must be installed on the device.
- You cannot create on-demand incidents for Juniper Networks QFX3000 Series and EX-XRE200 devices.

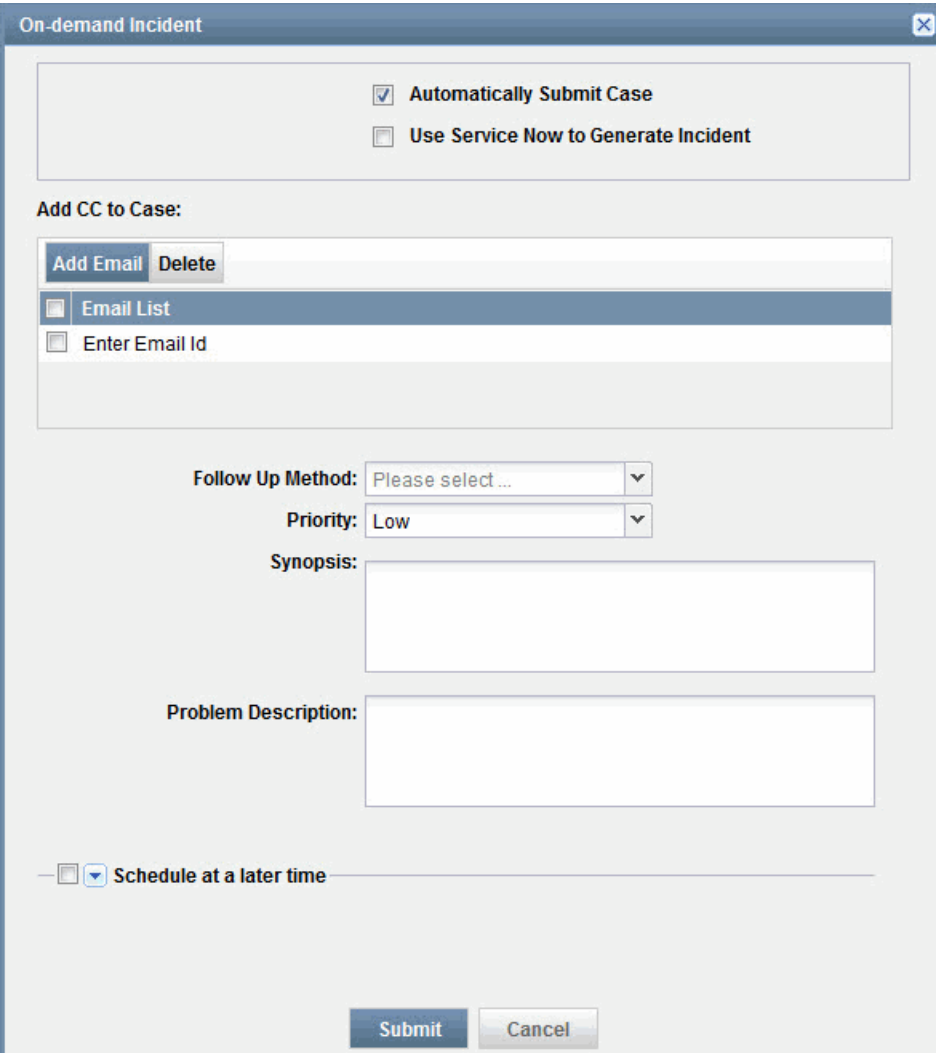
To generate on-demand incidents:

1. From the Service Now navigation tree, select **Administration > Service Now Devices**.
The Service Now Devices page appears.
2. On the Service Now Devices page, select the device for which you want to generate an on-demand incident.
3. From the Actions menu, select **Create On-Demand Incident**. Alternatively, right-click the device and select **Create On-Demand Incident**.

You can create on-demand incidents for up to five devices simultaneously.

The On-demand Incident dialog box appears as shown in [Figure 13 on page 98](#).

Figure 13: On-demand Incident Dialog Box



The dialog box is titled "On-demand Incident" and contains the following elements:

- At the top, there are two checkboxes: **Automatically Submit Case** (checked) and **Use Service Now to Generate Incident** (unchecked).
- Below this is a section labeled "Add CC to Case:" containing two tabs: "Add Email" and "Delete".
- Under the "Add Email" tab, there is a list with two items: "Email List" (selected) and "Enter Email Id".
- Below the list, there are two dropdown menus: "Follow Up Method:" (set to "Please select ...") and "Priority:" (set to "Low").
- Below the dropdowns are two text input fields: "Synopsis:" and "Problem Description:".
- At the bottom left, there is a checkbox labeled "Schedule at a later time" which is currently unchecked.
- At the bottom right, there are two buttons: "Submit" and "Cancel".

4. (Optional) At the top of the On-demand Incident dialog box, clear the **Automatically Submit Case** check box to avoid submitting incidents to JSS automatically.
5. (Optional) Select **Use Service Now to Generate Incident** to generate on-demand JMBs by using the Off-Box feature.
If you select this option, the Incidents page within Service Central displays the incident type as Off-Box for on-demand incidents.
6. Select the **Enter Email Id** check box to enter an e-mail ID in the user@example.com format.
7. (Optional) To add or delete multiple e-mail IDs, use the Add Email or Delete tabs respectively.
8. Select how updates about the case should be received from the **Follow Up Method** list. The available options are—Email Full Text Update, Email Secure Web Link, and Phone Call.

9. Select the priority of the case from the **Priority** list. The available options are—Critical, High, Medium, and Low. The default priority is **Low**.
10. In the **Synopsis** field, enter a synopsis of the on-demand incident.

The maximum number of characters allowed in the Synopsis field is 1028 characters.



NOTE: The values for the fields listed in steps 6 through 9 are already defined on the basis of the incident that is generated by the selected profile. You can modify these values if needed.

11. In the **Problem Description** field, enter a description of the RMA incident.

The maximum number of characters allowed in the Problem Description field is 1028 characters.

12. (Optional) If you want to schedule generating the on-demand incident at a later time, select the **Schedule at a later time** check box and enter the date and time for the schedule.
13. Click **Submit**.

A Job Information dialog box appears and displays the job ID.

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 (shown in Figure 14 on page 99), which displays information about the job such as the profile used in the incident, hostname, job status, and reason for the incident.

Figure 14: Create On-demand Incident Status Dialog Box

Profile Name	Host Name	Status	Reason
General	ex-4200-sn4	Failed	<p>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.</p> <p>Message from device : Details: Operational RPC Command Results Failed to open netconf channel domainId=0 deviceId=688250</p>

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Adding Devices from the Platform on page 90](#)
- [Deleting a Device on page 105](#)
- [Modifying Auto Submit Policy on page 106](#)
- [Viewing Exposure on page 96](#)

- [Collecting RSI and System Log Files on page 100](#)

Collecting RSI and System Log Files


Service Now provides the Configure File Collections option with which you can configure the interval for which a Request Support Information (RSI) command can be executed on a device and the output collected. For example, you can set the RSI command to be executed for every two hours. This prevents the RSI command from executing for each event that occurs on the device. Instead, the RSI command is executed only once during the configured interval to collect the information when an event occurs on the device.

The following example illustrates how RSI is collected:
In this example, the following considerations are made:

- Interval for executing RSI command: 1hr
- Time at which RSI was last executed: 1:00 PM

Time of Event	RSI Executed	Comment
1:30 PM	No	As the RSI command was last executed at 1:00 PM and the interval for executing the RSI command is set to 1hr, the RSI command is not executed again when an event occurs at 1:30 PM.
1:59 PM	No	
2:00 PM	Yes	As the RSI command was last executed at 1:00 PM and the interval for executing the RSI command is set to 1hr, the RSI command is executed again at 2:00 PM when an event occurs on the device.
2:01 PM	No	
4:30 PM	Yes	The RSI command is executed at 4:30 PM to collect the RSI.
4:35 PM	No	
5:30 PM	Yes	



NOTE: The  icon, if present in the device row (next to the device's organization), indicates that while copying a JMB from the device to Service Now, one or more JMB files, such as attachments or log files, are not deleted from the device.

If you place the cursor on the icon, the files that are not deleted appear. You must manually delete these files from the device.



NOTE: From AI-Script Release 4.0 onward, the attachment section of a JMB contains commands executed in response to an event and links that you can click to view or download the command output.

To configure the interval for collecting RSI and system log files:

1. In the Service Now navigation tree, select **Administration > Service Now Devices**.
The Service Now Devices page appears.
2. On the Service Now Devices page, select the device for which you want to collect RSI and system log files.
3. From the Actions menu, select **Configure File Collection**. Alternatively, right-click the device and select **Configure File Collection**.

The Collection of Files dialog box appears as shown in [Figure 15 on page 101](#).

Figure 15: Configure File Collections Dialog Box

Configure File Collections

These settings should not be changed without specific guidance from Juniper Networks. Changing these settings might result in loss of critical debug data or might affect the run time performance of the device.

RSI

- ☒ Do not change settings
- ☐ Use default setting
- ☐ Do not collect
- ☐ Always collect
- ☐ Minimum interval between RSI collection: 5 mins

Log Files

- ☒ Do not change settings
- ☐ Use default setting
- ☐ Do not collect
- ☐ Always collect

☒ Schedule 'Collection of Files' changes to be updated on device(s) at specified time: _____

Submit **Cancel**

4. In the RSI section of the Configure File Collections dialog box, select one of the following:

- **Do not change settings** to leave the settings for collecting RSI as is. This option is selected by default.

Using this dialog box, you can choose to configure the interval for collecting only the RSI or log files. If you want to configure collecting only the log files without changing the configuration for collecting RSI files, select this option.

For all devices, by default, Service Now is configured to collect RSI every five minutes. However, the following exceptions apply:

- Service Now is configured to collect RSI every 15 minutes for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.
- Service Now is configured to not collect RSI for the following devices:
 - ACX Series—ACX1000 and ACX1100
 - EX Series—EX2200 and EX3300
 - SRX Series—SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650
- **Use default setting** to collect RSI from the device for an event if five minutes have passed since RSI was last collected from that device
- **Do not collect** if you do not want to collect RSI for any event that occurs on the device
- **Always collect** to always collect RSI for all events that occur on the device
- **Minimum interval between RSI collection** to configure the minimum time interval for collecting RSI between consecutive events. If you select this option, select the time interval from the drop-down list provided below this option.

5. In the Log Files section of the Configure File Collections dialog box, select one of the following:

- **Do not change settings** to leave the settings for collecting system log files as is. This option is selected by default.

Using this dialog box, you can choose to configure the interval for collecting only the RSI or system log files. If you want to configure collecting only RSI without changing the configuration for collecting system log files, select this option. By default, Service Now is configured to collect system log files for every event.

- **Use default setting** to collect system log files for every event that occurs on the device
- **Do not collect** if you do not want to collect system log files for any event that occurs on the device
- **Always collect** to collect system log files for every event that occurs on the device

6. (Optional) If you want to schedule this configuration for a later time, select the **Schedule 'Collection of Files' changes to be updated on device(s) at specified time:** check box and select a date and time for the schedule from the list.

7. Click **Submit**.

A job is created to save the configuration and the job ID is displayed in the Job Information dialog box.

8. In the Job Information dialog box, click the *job ID* link to view the status of the job.

Related Documentation

- [AI-Scripts Overview](#)

Requesting RMA Incidents

You can use the Off-Box feature in Service Now to request RMA incidents for a device. With the Off-Box feature, RMA incidents are generated using the **directive.rc** file that is preloaded in Service Now. Currently, this feature is not supported on devices that are not associated with a device group. If Service Now operates in partner proxy mode, this feature is disabled for devices belonging to connected members.

To request an RMA incident for a device:

1. From the Service Now navigation tree, select **Administration > Service Now Devices**.
The Service Now Devices page appears.
2. On the Service Now Devices page, select the device for which you want to request an RMA incident.
3. From the Actions menu, select **Request RMA**. Alternatively, right-click the device and select **Request RMA**.



NOTE: Currently, Service Now supports requesting RMA incidents for only one device at a time.

The Request RMA page appears as shown in [Figure 16 on page 104](#).

Figure 16: Request RMA page

4. (Optional) At the top of the Request RMA page, clear the **Automatically Submit Case** check box if you do not want to submit RMA incidents automatically to JSS.
5. Under Email List, click the **Enter Email Id** check box to enter an e-mail ID in the user@example.com format.
6. (Optional) To add or delete e-mail IDs, use the Add Email or Delete buttons respectively.
7. From the **Follow Up Method** list, select the mode for receiving updates about the case.
The available options are—Email Full Text Update, Email Secure Web Link, and Phone Call.
8. From the **Priority** list, select the priority of the case.
The available options are—Critical, High, Medium, and Low. The default priority is Low.
9. In the **Synopsis** field, enter a synopsis of the RMA incident.
The maximum number of characters allowed in the Synopsis field is 1028 characters.
10. In the **Problem Description** field, enter a description of the RMA incident.
The maximum number of characters allowed in the Problem Description field is 1028 characters.
11. Select the address group from the **Address Groups** list.
The Address Groups list lists all the address groups configured in Service Now and None. None indicates that no address group is associated with this request.
12. Enter the address in the **Ship-to Address** field to which the device components or parts must be shipped.

13. Click the **Select Device Components** link.

The Device Physical Inventory Components page that appears displays the device parts with an option to select device parts or components. You can select and add device parts or components to be included in the Request RMA Parts field.

14. (Optional) If you want to schedule generating the on-demand incident at a later time, select the **Schedule at a later time** check box and enter the date and time for the schedule.
15. Click **Submit**.

The selected parts are populated in the **Request RMA Parts** field. You can verify the contents and then create the incident.

Related Documentation

- [Generating On-Demand Incidents on page 96](#)
- [Service Now Devices Overview on page 86](#)
- [Collecting RSI and System Log Files on page 100](#)

Deleting a Device

When you delete a device, the device is deleted from Service Now along with its related incidents and JMBs only from the Service Now database. The device is however not deleted from the Junos Space Platform.

To delete a device from Service Now:

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

The Service Now Devices page lists the Service Now devices.

2. Select the device that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.

The **Delete** dialog box prompts you to confirm the deletion.

3. Click **Delete**.

The selected device is deleted from the Service Now database and is no longer displayed on the Service Now Devices page.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Adding Devices from the Platform on page 90](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Modifying Device Groups on page 85](#)

Associating Devices with a Device Group

Using Service Now, you can associate devices with device groups which are associated with Service Now organizations. Associating devices with device groups helps you group devices under different site IDs.

If Service Now is configured to work in the Partner Proxy mode, you can combine devices that are directly managed by Service Now and devices from a connected member in a single Service Now device group. Alternately, you can create a device group for each connected member and associate them to Service Now organizations dedicated to each connected member. This kind of grouping enables you to track and organize technical support cases for a single end-customer using different organizations (site IDs).

To associate devices with device group:

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

The Service Now Devices page lists the Service Now devices.

2. Select the device that you want to associate with a device group and select **Associate Device Groups** from either the **Actions** list or the right-click menu.

The **Associate Device Groups** dialog box appears.

3. From the **Device Group** list, select the device group that you want to associate with the selected device.

4. Click **Submit**.

The device is associated with the selected device group. You can verify the changes on the Service Now Devices page, in the **Device Group** column.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Adding Devices from the Platform on page 90](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Modifying Device Groups on page 85](#)
- [Modifying Auto Submit Policy on page 106](#)

Modifying Auto Submit Policy

Auto submit policies enable devices to submit incidents that occur on them to JSS automatically. To assign auto submit policies to devices, you must first create them. For information on creating auto submit policies, see [“Creating an Auto Submit Policy” on page 136](#).

To modify an auto submit policy:

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

The Service Now Devices page appears.

2. Select the devices for which you want to assign auto submit policies, and select **Modify Auto Submit Policy** from either the **Actions** list or the right-click menu.

The **Modify Auto Submit Policy** dialog box appears and displays all the available auto submit policies and selected devices.

Figure 17: Modify Auto Submit Policy Page

Modify Auto Submit Policy

Select from the list below one or more Auto Submit Case Policies for the device(s) listed under Devices

Select Policy

☒ ASP

Selected Devices	Policy
mx-80-sn3	
snx-3600-sn1	
device1	
device2	ASP(disabled)
device3	

Add Remove Cancel

3. Select the auto submit policies that you want to assign to the selected devices.
4. To assign auto submit policies to selected devices, click **Add**.

To remove an assigned policy from the devices, select the policy and click **Remove**.

The Service Now Devices page appears. The Quick View area displays the policies a device is assigned with and the policy status (enabled or disabled).

5. (Optional) To verify your changes, navigate to Administration > Auto Submit Policy and view the list of devices to which the selected auto submit policies are assigned.

Related Documentation

- [Auto Submit Policy Overview on page 135](#)
- [Adding Devices from the Platform on page 90](#)
- [Service Now Devices Overview on page 86](#)
- [Collecting RSI and System Log Files on page 100](#)

Viewing Incidents

You can use Service Now to view the incidents that occur on the devices.

To view incidents:

1. From the Service Now navigation tree, select **Administration > Service Now Devices**.
The Service Now Devices page lists the Service Now devices.
2. Select a device to view the incidents that are detected on it.



NOTE: Currently, Service Now allows you to select only one device at a time.

3. Select **View incidents** from either the **Actions** list or the right-click menu.

The Incidents page displays the incidents detected for the selected device.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Adding Devices from the Platform on page 90](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Modifying Device Groups on page 85](#)
- [Collecting RSI and System Log Files on page 100](#)

Verifying Connection between Devices and FTP Server

Service Now uploads core files from devices to FTP server. Using service now, you can verify the connection between the devices and the FTP server. This feature is disabled for end-customer devices and also uploading to SFTP server is not supported.

To verify the connection between the device and the FTP server:

1. From the Service Now navigation tree, select **Administration > Service Now devices**. The Service Now Devices page appears.
2. Select the device for which you need to verify the FTP connection, and select **Check FTP Server** from either the **Actions** list or the right-click menu. The Check FTP Server Access dialog box appears.
3. Select the device, and click **Submit**. The Alert dialog box appears with the Job ID.
Click the *job ID* to go to the Job Management page and monitor the connectivity status.

Related Documentation

- [Service Now Devices Overview on page 86](#)
- [Uploading Core Files Generated for Events on page 133](#)
- [Updating Core File Upload Configuration on page 82](#)

Event Profiles and AI-Scripts

- [Event Profiles Overview on page 109](#)
- [Adding an Event Profile on page 110](#)
- [Cloning an Event Profile on page 114](#)
- [Deleting Event Profiles on page 116](#)
- [Viewing an Event Profile on page 116](#)
- [Pushing an Event Profile to Devices on page 117](#)

- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Setting an Event Profile as Default on page 120](#)
- [Exporting Events Data in Excel Format on page 120](#)
- [Adding a Script Bundle to Service Now on page 121](#)
- [Setting a Script Bundle as Default on page 122](#)
- [Deleting a Script Bundle from Service Now on page 122](#)

Event Profiles Overview

An event profile is a set of event scripts, selected from an AI-Scripts bundle that you want to install on Service Now devices.

To create an event profile, you need an AI-Scripts bundle from which you can select the event scripts that you want to include in an event profile. The set of event scripts in an event profile can be updated using the latest AI-Scripts bundle.

The latest AI-Scripts bundle is pre-loaded with Service Now and hence when you install Service Now, the latest AI-Scripts bundle is displayed on the Script Bundles page. You can also download other AI-Scripts bundles from the Juniper Networks software download site and upload them to Service Now (see [“Adding a Script Bundle to Service Now” on page 121](#)).

Service Now has a default event profile and an AI-Scripts bundle. The default event profile is always associated with an AI-Scripts bundle. For new Service Now installs or upgrades, the default event profile is associated with the preloaded AI-Scripts bundle.

After installing or upgrading Service Now, you can add additional AI-Scripts bundles and set any AI-Scripts bundle and event profile as the default. The default AI-Scripts bundle is automatically selected while creating a new event profile and the default event profile is automatically selected while installing an event profile on devices.



NOTE: Read the KB article, <http://kb.juniper.net/KB19155>, before installing AI-Scripts on devices.

Service Now allows you to clone an existing event profile by modifying its name, description, the associated AI-Scripts bundle, set of included event scripts, and event script priorities. Cloning an event profile allows you to make changes without losing the original event profile. After you make your modifications, you can save the cloned event profile and install it on devices on which the original event profile is installed. You can also install the new event profile on any other devices. The priority of event scripts determine the priority shown in the JMBs generated for a Service Now event. After you install event profiles on devices, you can filter and display only those devices on which a specific event profile is installed. Service Now also enables you to export event data that is specific to an event profile to Excel format and delete event profiles that are not associated with devices.

In Service Now, event profiles are displayed on the Event Profiles page ([Figure 18 on page 110](#)). The tabular view of the Event Profiles page displays information

about the event profile including the total number of incidents generated per event in the event profile, the total number of active events, the total number of inactive events, the number of devices on which the event profile is installed, most active events, least active events, and inactive events. The default event profile is indicated by a unique icon as shown in [Figure 18 on page 110](#), Base_Profile_3_7R1_2 is the default event profile. a

Figure 18: View Event Profiles Page

Name	Description	AI Script Version	Created By	Created	Events Included	Events Excluded	Devices
Copy of Base_Profile_3_7R1_2	Base Profile for Bundle Version: 3.7R1.2	3.7R1.2	super	Oct 4, 2013 1:28:39 PM IST	433	0	0
Copy of Profile name		3.7R1.2	super	Oct 3, 2013 4:10:58 PM IST	433	0	0
Profile name		3.7R1.2	super	Oct 3, 2013 4:09:06 PM IST	433	0	1
Base_Profile_3_7R1_2	Base Profile for Bundle Version: 3.7R1.2	3.7R1.2	Service Now	Jul 30, 2013 12:52:01 PM IST	433	0	2

Using the **Event Profiles** workspace, you can perform the following tasks:

- Add an event profile
- Push an event profile to devices
- Display devices associated with an event profile
- Set an event profile as default
- Export events data to Excel format
- View an event profile
- Clone an event profile
- Delete event profiles

Related Documentation

- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Adding an Event Profile on page 110](#)
- [Pushing an Event Profile to Devices on page 117](#)
- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Setting an Event Profile as Default on page 120](#)
- [Exporting Events Data in Excel Format on page 120](#)
- [Viewing an Event Profile on page 116](#)
- [Cloning an Event Profile on page 114](#)
- [Deleting Event Profiles on page 116](#)

Adding an Event Profile

An event profile is a set of scripts that are selected from an AI-Scripts bundle. Using event profiles, you can specify the event scripts you want to install on the devices. To add an event profile, you can use the default AI-Scripts bundle that is available when you install Service Now, or upload and use a new AI-Scripts bundle (see [“Adding a Script Bundle to Service Now” on page 121](#)).

After you add an AI-Scripts bundle to Service Now, to be able to install the AI-Scripts bundle on the devices, you must create an event profile using this AI-Scripts bundle.

To add an event profile:

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

The Add Event Profile page appears as shown in [Figure 19 on page 111](#).

Figure 19: Add Event Profile Page

The screenshot shows the 'Add Event Profile' page. It has a form with the following fields: 'Profile Name' (containing 'Test Profile'), 'Description', 'Script Bundle' (a dropdown menu showing 'jais-3.7R1.0-signed.igz'), and 'Find Events' (a search bar). There is an 'Add Script Bundle' button next to the Script Bundle dropdown. Below the form is a table titled 'Event Synopsis'. The table has columns: 'Event Synopsis', 'Type', 'Sub Type', 'Priority (editable)', 'KB Article', and 'RMA Event'. The table lists several events under categories like 'ACCT (1 Item)', 'ALARM (4 Items)', and 'ASP (2 Items)'. At the bottom of the page are 'Submit' and 'Cancel' buttons.

Event Synopsis	Type	Sub Type	Priority (editable)	KB Article	RMA Event
Category: ACCT (1 Item)					
ACCT_XFER_POPEN_FAIL	Software Failure	Communication Error	Medium	View KB	No
Category: ALARM (4 Items)					
CONNECTION_SEND_ERROR	Software Failure	Process error	Medium	View KB	No
CONNECTION_RTLOGD_FAIL	Software Failure	Initialization error	Medium	View KB	No
CONNECTION_CRAFTD_FAIL	Software Failure	Initialization error	Medium	View KB	No
CONNECTION_CHASSISD_FAIL	Software Failure	Initialization failure	High	View KB	No
Category: ASP (2 Items)					
ASP_IDS_INV_CLEAR_QUERY_VER	Software Failure	Unexpected output	High	View KB	No
ASP_IDS_INV_CLEAR_QUERY	Software Failure	Unexpected output	High	View KB	No
Category: ASP_L2TP (1 Item)					

For a description of the fields displayed on this page, see [Table 13 on page 111](#).

Table 13: Add Event Profile Page Field Descriptions

Field	Description
Profile Name	Enter a name of the event profile. The name can contain alphanumeric characters, underscore, hyphens and space. The maximum number of characters allowed is 255.
Description	Enter a description for the event profile. The maximum number of characters allowed is 255.
Script Bundle	Lists the AI-Scripts bundles that are available in Service Now. This consists of the default AI-Scripts bundle that is available with Service Now and the ones that you upload.
Find Events	Specify an event from the list to filter the displayed list of events
Show Selected Events	Shows all the events that you have selected.
Description of the columns in the Add Event Profiles page	
Event Synopsis	Name used to identify the event script.

Table 13: Add Event Profile Page Field Descriptions (*continued*)

Field	Description
Type	Type of event that triggers the event script: <ul style="list-style-type: none"> • Hardware failure • Software failure • Resource Exhaustion
Sub Type	A brief description of the event type that triggers the event script to execute. For example, file system error, communication error, socket failure, excessive memory utilization, database failure, session error, memory allocation error, initialization error, process error, and so on.
Priority	Priority level of the event script. The values are: <ol style="list-style-type: none"> 1. Low 2. Medium 3. High 4. Critical
KB Article	Provides a link to knowledge base where you can find information such as cause and solution for the event..
RMA Event	Specifies if this is an RMA event or not.

2. Enter an event profile name.
3. (Optional) Enter a description for the event profile.
4. Select a script bundle from the **Script Bundle** list.

By default, the script bundle that is set as the default is automatically selected and you can modify this selection if required.
5. (Optional) To add a new script bundle, click **Add Script Bundle** (see [“Adding a Script Bundle to Service Now” on page 121](#)).
6. (Optional) To look for specific events, use the **Find Events** field.
7. Click **Submit**.

An event profile is created with your specifications and the Save Event Profile dialog box appears.

8. Click one of the following links based on the required results.

Link	Result
Apply this profile to original set of devices	The Potential Exposure to Known Issues page appears and displays information about the selected set of devices. A bang (!) icon is placed next to devices that risk the chance of exposure.

Figure 20: Potential Exposure to Known Issues Page

Potential Exposure when Event Profile is installed on Devices				
Device Name	Serial Number	Product	Version	Exposure
ex-2200-sn3	C1W0210403356	EX2200-24T-4G	12.2R3.5	Click

- (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
- (Optional) To view a device's exposure to known issues, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated with the respective device.
Click **Return to Potential Exposure** to continue.
- Click **Continue**.
A confirmation pop-up box lists the final list of devices on which the selected event profile must be installed.
You can remove devices from the list by clearing the check boxes of the devices you want to delete.
- Click **Install**.
The selected event profile is installed on the devices with which it is associated, and the Service Now Devices page appears.

Apply this profile to devices manually	<p>The Push to Devices page appears. Here you can select Service Now devices on which you want to install the event profile.</p> <p>For more information, see "Pushing an Event Profile to Devices" on page 117 .</p>
Return to the Profiles Page	The event profile installation task is canceled, and the Event Profiles page appears.

Related Documentation

- [Pushing an Event Profile to Devices on page 117](#)
- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Event Profiles Overview on page 109](#)

Cloning an Event Profile

Service Now enables you to clone an existing event profile and modify its priority to create another event profile. After you clone an event profile, you can redeploy the event profile, or deploy the event profile on new devices. When you create a clone of an event profile, the event profile name is appended with **Copy of**.



NOTE: Editing an event profile is similar to cloning an event profile. You cannot directly edit an event profile.

To clone an event profile:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. Select the event profile that you want to clone, and select **Clone** from either the **Actions** list or the right-click menu.

The **Clone Event Profile** dialog box displays the attributes of the event profile that you have selected.
3. Select the events that you want to include in the cloned event profile.
4. (Optional) To search for specific events, enter the name of the event in the **Find Events** field.
5. (Optional) Click the **Priority** field to modify the event priority. The values are:
 1. Low
 2. Medium
 3. High
 4. Critical

6. Click **Submit**. The event profile is created and the **Save Event Profile** dialog box appears.
7. Click one of the following links based on the required results.

Link	Result
Apply this profile to original set of devices	<p>When you click this link, the Select Devices to Install Profile page appears.</p> <p>In this page, you must</p> <ul style="list-style-type: none"> Specify the devices on which you want to install the event profiles by selecting the check box provided next to each device. To specify all the listed devices, select the check box present next to Organization column heading. Specify if the AI-Scripts bundle files should not be stored in the device by selecting the Never Store Script Bundle files on device check box. If this check box is selected, roll back to this version of the AI-Scripts bundle is not possible in future. Specify if the AI-Scripts bundle files should be deleted from the device after successful installation of the event profile. If the Remove Script Bundle files after successful install check box is selected, the AI-Scripts bundle files are deleted from the device after the installation of the event profile. If you want to install the event profiles later on the devices, schedule the installation. Selecting the Schedule at a later time check box provides the controls to specify the date and time of the installation. <p>Click Submit to proceed with the installation. The Potential Exposure when Event Profile is Installed on Devices page displays the selected set of devices. A bang (!) icon present next to a device indicates that the device is susceptible to events in the event profile.</p> <p>In this page, you can</p> <ul style="list-style-type: none"> Export information on devices susceptible to events. To export device data in an Excel format, click Export Devices with Exposure to Excel. View the events to which a device is susceptible. To view the events to which a device is susceptible, click the respective link displayed in the Exposure column. The View Exposure page appears and displays the known issues associated with the respective device. Click Return to Potential Exposure to continue. <p>To proceed with the installation:</p> <ol style="list-style-type: none"> Select the devices on which you want install the event profile and click Continue. The Install Event Profile dialog box appears. Click Install or Cancel to confirm or cancel the installation of the event profiles on the selected devices.
Apply this profile to devices manually	<p>When you click this link, the Push to Devices page appears. Here you can select Service Now devices on which you want to install the event profile.</p> <p>For more information, see "Pushing an Event Profile to Devices" on page 117.</p>
Return to the Profiles Page	<p>When you click this link, the event profile installation task is canceled, and the Event Profiles page appears.</p>

Related Documentation • [Pushing an Event Profile to Devices on page 117](#)

- [Event Profiles Overview on page 109](#)

Deleting Event Profiles

Using Service Now, you can delete multiple event profiles. You can delete an event profile only if it is not associated with a device.



NOTE: When you delete a default event profile, the latest created profile is automatically set as the default.

To delete event profiles:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. Select the event profiles that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.
The **Delete Event Profiles** dialog box displays the list of selected event profiles.
3. Click **Delete** to confirm.
The selected event profiles are deleted. Verify the deletion by To verify, you can check the list of event profiles displayed on the Event Profiles page.
4. Check the Event Profiles page to verify the deletion.

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Cloning an Event Profile on page 114](#)
- [Pushing an Event Profile to Devices on page 117](#)

Viewing an Event Profile

Using Service Now, you can view an event profile's name, its description, and the scripts that are associated with it.

To view the event scripts that are part of an event profile:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. Select the event profile whose details you want to view, and select **View Events** from either the **Actions** list or the right-click menu.

The View Events page displays the event profile's name, its description, and the scripts that are associated with it. The event script details includes the names of the event scripts, types, subtypes, priorities, link to knowledge base about the event, if the event is a RMA event occurrences in the last 90 days, the total number of occurrences till date, the number of unique devices, and the number of top devices.

- Click **OK** to return to the Event Profiles page.

Related Documentation

- [Exporting Events Data in Excel Format on page 120](#)
- [Cloning an Event Profile on page 114](#)
- [Pushing an Event Profile to Devices on page 117](#)

Pushing an Event Profile to Devices

An event profile is a set of event scripts that are selected from an AI-Scripts bundle. When you push an event profile onto Juniper Networks devices, these event scripts are installed on the devices. The event scripts automatically detect and report problems (incident) that occur on the device and also provide monitoring information. Service Now uses Device Management Interface (DMI) to install and remove event profiles on devices. DMI is an extension to the NETCONF network management protocol.

When you install event profiles on individual systems (chassis) with dual Routing Engines, Service Now installs the event profiles on both the primary and backup Routing Engines.



NOTE: While operating in partner-proxy mode, you cannot install event profiles to a connected member's device.

To install an event profile on devices:

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

The Event Profiles page appears.

- Select the event profile that you want to push to devices, and select **Push to devices** from either the **Actions** list or the right-click menu.

The **Push to Devices** dialog box appears (see [Figure 21 on page 117](#)).

Figure 21: Push to Devices Dialog Box

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle	Event Profile
JCare-Plus	Default for JCare-Plus	device1	PW0213250012	ACX1100	12.3X51-D10.5	3.7R1.2	Base_Profile_3_7R1_2
JCare-Plus	Default for JCare-Plus	device2	JN11B7992AEA	M120	11.4R7.5	3.7R1.2	Profile name
JCare-Plus	Default for JCare-Plus	device3	33108	M101	11.4R7.5	3.7R1.2	Base_Profile_3_7R1_2
JCare-Plus	Default for JCare-Plus	device4	NK0212350232	ACX2100	12.3X52-D10.4		
JCare-Plus	Default for JCare-Plus	device5	AB3510AA0021	SRX3600	11.4R9.4		
JCare-Plus	Default for JCare-Plus	device6	73682	M40E	11.4R7.5		
JCare-Plus	Default for JCare-Plus	device7	E4008	MX80-48T	11.4R8-S2		

Page 1 of 1

Displaying 1 - 7 of 7

☐ Never store Script Bundle files on device (if selected roll-back option will not be available)

☐ Remove Script Bundle files after successful install

☐ Schedule at a later time

Submit Cancel



NOTE: You can install event profiles only on devices for which you can specify correct login credentials and that belong to a device group.

3. Select the devices on which you want to install the event profile.
4. (Optional) If you do not want to save a copy of the event profile after it is installed on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.
5. (Optional) If you want to remove the script bundle from the device after it is installed, select the **Remove Script Bundle files after successful install** check box.
6. (Optional) If you want to schedule a time for installation, select the **Schedule at a later time** check box, and specify the **Date and time** for the installation. The installation process begins automatically at the time you specify.
7. Click **Submit**.

The Potential Exposure when Event Profile is Installed on Devices page appears and displays information about the selected set of devices. A bang (!) icon is placed next to devices that are susceptible to the events in the event profile.

Figure 22: Potential Exposure to Known Issues Page

Potential Exposure when Event Profile is installed on Devices					
					Export Devices with Exposure to Excel
<input type="checkbox"/>	Device Name	Serial Number	Product	Version	Exposure
<input checked="" type="checkbox"/>	ex-2200-sn3	CW0210403356	EX2200-24T-4G	12.2R3.5	Click

8. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
9. (Optional) To view the events to which the device is susceptible, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated for the respective device.
10. Click **Return to Potential Exposure** to continue.
11. To proceed with the installation, Click **Continue**.

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

12. Click **Install**.

The event profile installation task is performed when scheduled and the **Job Information** dialog box displays the job ID.

To view the status of this task, click the *job ID* link. The Jobs page displays the status of the job. The **Device Details** dialog box also displays the status of script installation on the selected devices.

If you have installed the event profile on a dual Routing Engine, the results displayed on the Jobs page shows 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.

13. Click **OK**.

The View Event Profiles page appears.

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Event Profiles Overview on page 109](#)
- [Adding an Event Profile on page 110](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Cloning an Event Profile on page 114](#)
- [Viewing Exposure on page 96](#)

Displaying Devices Associated with an Event Profile

Using Service Now, you can view only those devices that are associated to a specific event profile. This task is disabled when you select an event profile that is not associated to any device.

To display devices associated to an event profile:

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

The Event Profiles page appears.

2. Select the event profile to view the devices associated with it, and select **Show Associated Devices** from either the **Actions** list or the right-click menu.

The Service Now Devices page displays only the devices that are associated with the event profile that you selected.

Related Documentation

- [Viewing an Event Profile on page 116](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)
- [Adding an Event Profile on page 110](#)
- [Pushing an Event Profile to Devices on page 117](#)

Setting an Event Profile as Default

Service Now allows you to set an event profile as the default. When you select devices on which you want to install an event profile, the default event profile is automatically selected as the event profile that must be installed. The default event profile is represented by a unique icon on the View Event Profiles page. If you delete the default event profile, the latest event profile created is automatically set as the default.

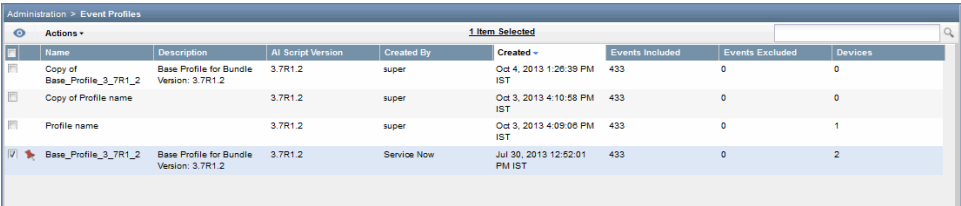
To set an event profile as the default:


1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. Select the event profile that you want to set as the default, and select **Set as Default Profile** from either the **Actions** list or the right-click menu.

The **Set As Default Profile** dialog box prompts you for confirmation.

3. Click **Confirm**.
The selected event profile is set as the default and is automatically selected as the event profile that must be installed when you select devices in the Service Now Devices page for installing event profile. The default event profile (for example, `Base_Profile_3_7R1_2` in [Figure 23 on page 120](#)) shows the default event profile indicated by a unique icon.

Figure 23: View Event Profiles Page



Name	Description	AI Script Version	Created By	Created	Events Included	Events Excluded	Devices
Copy of Base_Profile_3_7R1_2	Base Profile for Bundle Version: 3.7R1.2	3.7R1.2	super	Oct 4, 2013 1:20:39 PM IST	433	0	0
Copy of Profile name		3.7R1.2	super	Oct 3, 2013 4:10:58 PM IST	433	0	0
Profile name		3.7R1.2	super	Oct 3, 2013 4:09:06 PM IST	433	0	1
 Base_Profile_3_7R1_2	Base Profile for Bundle Version: 3.7R1.2	3.7R1.2	Service Now	Jul 30, 2013 12:52:01 PM IST	433	0	2

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Cloning an Event Profile on page 114](#)
- [Pushing an Event Profile to Devices on page 117](#)

Exporting Events Data in Excel Format

Service Now enables you to export data such as the number of times a particular event occurred in the devices in the last 7 days, 30 days, 365 days, events that never occurred, and the day on which new events occurred to an Excel file and save it on your local file system.

To export events data to an Excel file:

1. From the Service Now navigation tree, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. Double-click the event profile whose event activity you want to export to an Excel file.

The **Event Profile Detail** dialog box displays details about the event activity that are associated to the event profile that you selected.

3. Click the **Export events to Excel** link.
The browser dialog box allows you to open or save the Excel file.
4. To open the Excel file, select **Open with**.
To save the Excel file, select **Save File** and navigate to the folder in your local file system. Click **Save** in the browser dialog box to save the Excel file.
5. Click **OK**.
The event activity information that appears in the Event Profile Detail dialog box is contained in five separate worksheets in the Excel file.

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 119](#)
- [Cloning an Event Profile on page 114](#)
- [Pushing an Event Profile to Devices on page 117](#)

Adding a Script Bundle to Service Now

The Script Bundles page provides a central point for managing script bundles (also known as AI-Scripts install packages) downloaded from the Juniper Networks software download site. The script bundles must be stored locally to the system running the Service Now application. You need Service Now Administrator privileges to add a script bundle.

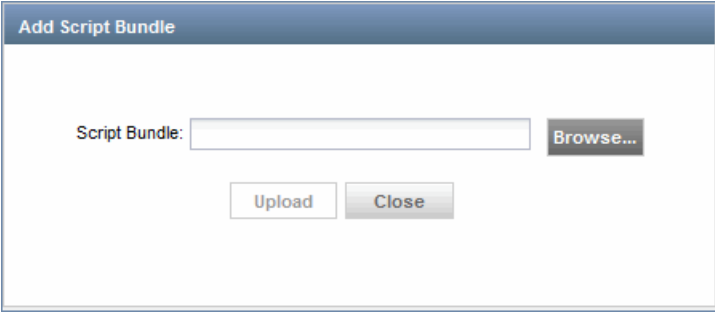
After you add a script bundle to Service Now, to be able to install the script bundle on devices, you must first create an event profile using this script bundle. See [“Adding an Event Profile” on page 110](#).

To add a script bundle:

1. From the Service Now taskbar, select **Administration > Event Profiles > Script Bundles > Add Script Bundle**.

The Add Script Bundle page appears as shown in [Figure 24 on page 121](#).

Figure 24: Add Script Bundle Dialog Box



2. Click **Browse**.

The File Upload window appears.

3. Locate the script bundle and click **Upload**.

The selected script bundle is uploaded to Service Now and appears on the Script Bundles page.

Related Documentation

- [AI-Scripts Overview on page 21](#)
- [Deleting a Script Bundle from Service Now on page 122](#)
- [Installing an Event Profile on Devices Using Service Now on page 91](#)

Setting a Script Bundle as Default

Service Now allows you to set a script bundle as the default. When you create an event profile, the default script bundle is automatically selected as the script bundle from which you select event scripts to associate with the event profile. The default script bundle is represented by a unique icon on the Script Bundles page. If you delete the default script bundle, the latest uploaded script bundle is automatically set as the default.

To set a script bundle as the default:

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

The Script Bundles page lists the available script bundles.

2. Select the script bundle that you want to set as the default, and select **Set as Default Bundle** from either the **Actions** list or the right-click menu.

The Set as Default Bundle dialog box prompts you to confirm.

3. Click **Confirm**.

The selected script bundle is set as the default and is represented by a unique icon on the Script Bundles page.

Related Documentation

- [Manually Installing AI-Scripts on Devices on page 29](#)
- [Adding a Script Bundle to Service Now on page 121](#)
- [Deleting a Script Bundle from Service Now on page 122](#)

Deleting a Script Bundle from Service Now

With Service Now Administrator privileges, you can delete script bundles.



NOTE: You cannot delete the pre-loaded script bundle that is available with Service Now.

To delete a script bundle:

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

The Script Bundles page lists the available script bundles.

2. Select the script bundle that you want to delete, and select **Delete Script Bundles** from either the **Actions** list or the right-click menu.

The Delete AI-Scripts dialog box prompts you to confirm the deletion.

3. Click **Delete**.

Service Now deletes the script bundle from the database and returns to the Script Bundles page.

Related Documentation

- [AI-Scripts Overview on page 21](#)
- [Adding a Script Bundle to Service Now on page 121](#)

Global Settings

- [Configuring Global Settings on page 123](#)
- [Adding an SNMP Server on page 129](#)
- [Editing and Deleting an SNMP Server on page 131](#)
- [Managing SNMP Traps on page 131](#)
- [Configuring Proxy Server Settings on page 132](#)
- [Uploading Core Files Generated for Events on page 133](#)

Configuring Global Settings

You can use the Service Now global settings to perform the following tasks:

- Connect to Juniper Support Systems (JSS) and verify the connection status.
- Connect to Service Now partner and verify the connection status if Service Now is operating in End Customer mode.
- Share information with Juniper Networks about Service Now incidents and Service Now devices.



NOTE: You must have Service Now Administrator privileges to configure global settings.

For more information about standard, partner proxy, and end customer modes, see [“Service Now Modes” on page 42](#).

Using the Service Now Global Settings page, a Service Now end customer can connect to a partner’s Service Now application. When the Service Now application of an end customer connects to that of a partner, Junos Space uses a self-signed security certificate. Although, Junos Space does not trust this method of identification, it automatically accepts the certificate to ensure that the communication between the partner and the end customer is encrypted. After you connect to the partner’s Service Now application,

you enter End Customer mode. After Service Now begins to operate in End Customer mode, you cannot revert to Standard or Partner Proxy mode. After you connect to the Service Now application, you can add an organization using the credentials provided by the partner. For information about adding an organization, see [“Adding an Organization” on page 75](#). After the connection of the organization is validated, you can submit incidents and iJMBs to and open cases with the Service Now partner.

If you select the **Share Service Now Profile Information** option on the Global Settings page, you can periodically send data related to incident activities, devices under management, event policies, and Junos Space operations to JSS. Service Now uploads the data in an XML file and sends the XML file to JSS using MetadataUploadRequest. These files are uploaded to JSS once a week.

Information about the following elements is collected in the XML file. For more details, see [Table 14 on page 124](#).

- Fabric
- Application summaries
- Devices
- Organization
- Event profiles
- Incidents

Table 14: XML File Information

Element	Description
SpaceInfo	Specifies Junos Space information
FabricInfo	Specifies fabric information available in Junos Space
<ul style="list-style-type: none"> • RowID • Name of the fabric node • Status • CPU • RAM • Disk • AppLogic • Database • LoadBalancer • HardwareModel • SoftwareVersion • IsMasterNode • IsVIPNode • Date 	<ul style="list-style-type: none"> • ID of the element • Name of the fabric node • Status of the fabric node • Percentage of CPU used by the fabric node • Percentage of RAM used by the fabric node • Percentage of disk used by the fabric node • Ability to interact with devices • Status of the database in the fabric node • Status of the fabric node in load balancing • Hardware model of the fabric node • Software version installed in the fabric node • This value is set to true only if the fabric node is the primary node. • This value is set to true only if the fabric node is a Web IP node. • Date and time of collecting the fabric information

Table 14: XML File Information (*continued*)

Element	Description
ApplicationSummary <ul style="list-style-type: none"> • Application • RowID • AppName • AppVersion • ReleaseType • Build • IsEnabled • Date 	Specifies information about the applications installed on Junos Space <ul style="list-style-type: none"> • Container tag for application information • ID of the element • Name of the application • Version of the application • Release type of the application • Build number of the application • This value is set to true only if the application is enabled in Junos Space. • Date and time of collecting application summary information
DevicesInfo <ul style="list-style-type: none"> • Device • RowID • OSVersion • Product • SchemaVersion • ConnectionStatus • PrimarySiteID • SiteID • AIScriptVersion • IsManagedBySN • ProfileName • SerialNumber • RoutingEngine 	Specifies Information about the devices managed by Junos Space Network Management Platform <ul style="list-style-type: none"> • Container tag for device information • ID of the element • Version of Junos OS installed on the device • Product type of the device • Version of the Junos OS schema • Status of the connection between Junos Space and the device • Default site ID of the organization to which the device belongs • Site ID of the organization to which the device belongs • Version of AI-scripts installed on the device • This value is set to true only if the device is managed by Service Now. • Name of the event profile installed on the device • Serial number of the device • In case of dual Routing Engines, this element specifies the primary Routing Engine
ApplicationDetails <ul style="list-style-type: none"> • Application name 	Specifies detailed information about the application installed in Junos Space. Currently, only Service Now is supported. <ul style="list-style-type: none"> • Name of the application
OrganizationInfo <ul style="list-style-type: none"> • TotalConnectedMembers • Organization • RowID • Name • PrimarySiteID • SecondarySiteIDs • UserName • ConnectionStatus • JMBFilterLevel • Status • IsConnectedMember 	Specifies Information about the organizations in Service Now <ul style="list-style-type: none"> • Total number of connected members for the Service Now Partner • Container tag for organization information • ID of the element • Name of the organization • Primary site ID of the organization • List of secondary site IDs of the organization • Username of the organization • Connection status of the organization • Filter level of the JMB • Case submission status • This value is set to true only if it is a connected member.

Table 14: XML File Information (*continued*)

Element	Description
EventProfilesInfo	Specifies information about the event profiles installed in devices
<ul style="list-style-type: none"> EventProfile RowID Name EventsIncluded EventsExcluded AIScriptVersion TotalEventsInBundle EventsWithNoIncidents TotalIncidents AssociatedDevicesCount EventsInfo 	<ul style="list-style-type: none"> Container tag for event profile information ID of the element Name of the event profile that is installed Total number of events included in the event profile Total number of events excluded from the event profile AI-Scripts bundle version from where the profile is created Total number of events in the AI-Scripts bundle Total number of events in the profile for which no incidents are reported to Service Now Total number of incidents in Service Now for this profile Total number of devices in which this event profile is installed List of events present in this event profile
IncidentsInfo	Information about incidents in Service Now that are in the initial state
<ul style="list-style-type: none"> Incident RowID ID Synopsis ProblemDescription Organization PrimarySiteID SiteID Priority Severity Type DefectType EventType DeviceSerialNumber Release Version Product Platform 	<ul style="list-style-type: none"> Container tag for incident information ID of the element.. Incident ID. This is a CDATA section. Incident synopsis. This is a CDATA section. Problem description of this incident Name of the organization with which this device is associated in Service Now Primary site ID of the organization to which this device belongs Site ID of the organization to which this device belongs Priority of the incident Severity of the incident Type of the incident Type of defect that caused this incident Event type that caused this incident Serial number of the device on which this incident occurred Junos OS release installed on the device Junos OS release version installed on the device Product type of the device Platform type of the device

Table 15 on page 126 describes the command buttons on the Global Settings page.

Table 15: Global Settings Command Buttons


Button Name	Description	Enabled/Disabled	Results
	Help icon for the Global Settings page	Enabled if you have administrator privileges	Displays information collected for the metadata

Table 15: Global Settings Command Buttons (*continued*)

Button Name	Description	Enabled/Disabled	Results
Submit	Saves any modified Service Now global setting values and updates the Service Now application with these new values	Enabled if you have administrator privileges	Saves settings that were modified
Test Connection	<ul style="list-style-type: none"> In standard and Partner Proxy modes, verifies the organization's connectivity with JSS In End Customer mode, verifies the organization's connectivity with the partner's Service Now application 	Enabled if you have administrator privileges	Displays the Connection Status as Success or Failed
Cancel	Withdraws the submission of modified settings	—	Navigates back to the Global Settings page without saving the entries

To configure Service Now global settings:

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

The Global Settings page appears as shown in [Figure 25 on page 127](#).

Figure 25: Global Settings Page

2. Enter values for the global settings as described in [Table 16 on page 128](#).
3. Click **Submit** to save the global settings and update Service Now. Click **Cancel** to navigate back to the Global Settings page without saving the entries.

If you click the information icon displayed next to the Global Settings page heading, the Help page for global settings is displayed. This Help page contains the data related to sharing profile information.

[Table 16 on page 128](#) describes the fields displayed in the tabular view of the Global Settings page.

Table 16: Global Settings Parameters

Name	Description	Range/Length	Default
Outbound e-mail address	E-mail address that the recipients of mails from Service Now see (for example, <code>exampleservicenow@juniper.net</code>)		
Device Snapshot Purge Time (in days)	Number of days the device snapshots are stored in the Service Now database before they are deleted	<ul style="list-style-type: none"> • Never • 90 • 120 • 180 • 365 	180
Incident Purge Time (in days)	Number for of days the incidents are stored in the Service Now database before they are deleted.	<ul style="list-style-type: none"> • Never • 90 • 120 • 180 • 365 	365
Repeat Incident Dampening Period	<p>The time period for which no JMB is generated when the same event recurs on the device.</p> <p>This value can be overridden by configuring a dampening period for each event in the Auto Submit Policy.</p> <p>For information about the Auto Submit Policy, see "Creating an Auto Submit Policy" on page 136</p>	<ul style="list-style-type: none"> • None • Always • 1hr to12hr • 24hr • 48hr • 72hr • 96hr • 120hr 	None
Share Service Now Profile Information	<p>If this check box is selected, all the Service Now-related information is shared with JSS for tracking purposes.</p> <p>This option is not applicable in Offline mode.</p>		Service Now related information is shared with JSS
Collect Log Files	<p>If this check box is selected, log files are collected from all the Service Now devices.</p> <p>This behavior is overridden by log collection settings configured on individual Service Now devices.</p>		Logs are collected from Service Now devices

Table 16: Global Settings Parameters (*continued*)

Name	Description	Range/Length	Default
Connection Status	<p>Status of connection from Service Now to JSS.</p> <p>If Service Now is operating in End Customer mode, the connection status between Service Now and the partner proxy appears.</p>	<ul style="list-style-type: none"> • Success • No route to host • Connection refused • The Home Base server is temporarily unable to service your request 	

- Related Documentation**
- [Service Now Modes on page 42](#)
 - [Organizations Overview on page 73](#)
 - [Adding an SNMP Server on page 129](#)
 - [Editing and Deleting an SNMP Server on page 131](#)
 - [Configuring Proxy Server Settings on page 132](#)
 - [Managing SNMP Traps on page 131](#)

Adding an SNMP Server

You can specify a destination for SNMP traps to be sent when a Service Now notification policy is triggered. SNMP traps are sent to these destination only when the notification policy specifies this action. In **Service Now > Administration > Global Settings > SNMP Configuration**, the specified trap destinations are displayed.

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

To add an SNMP server:

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

The SNMP Servers page appears.

2. Click **Add**.

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

A screenshot of a 'Add SNMP Server' dialog box. It contains five input fields: 'Name' (empty), 'SNMP Server' (empty), 'UDP Port' (162), 'Community String' (empty), and 'Protocol Version' (v1). At the bottom are 'Add' and 'Cancel' buttons.

Add SNMP Server

Name:

SNMP Server:

UDP Port:

Community String:

Protocol Version:

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

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

Loading MIBs

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

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

Related Documentation

- [Configuring Global Settings on page 123](#)
- [Editing and Deleting an SNMP Server on page 131](#)
- [Configuring Proxy Server Settings on page 132](#)

Editing and Deleting an SNMP Server

SNMP servers are the destination for SNMP traps to be sent when a Service Now notification policy is triggered. You can modify the parameters of these SNMP servers and also delete them.

Editing an SNMP Server

To edit an SNMP server:

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

The SNMP Servers page appears.

2. Select the SNMP server whose parameters you want to modify.
3. Click **Edit**.
The **Edit SNMP** dialog box appears.
4. Make the desired changes to the parameters.
5. Click **Save**.

The changes are saved in the Service Now database. To verify, you can view the changes on the SNMP Servers page.

Deleting an SNMP Server

To delete an SNMP server:

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

The SNMP Servers page appears.

2. Select the SNMP server that you want to delete.
3. Click **Delete**.

The selected SNMP server is deleted from the Service Now database and is no longer displayed on the SNMP Servers page.

Related Documentation

- [Configuring Global Settings on page 123](#)
- [Adding an SNMP Server on page 129](#)
- [Configuring Proxy Server Settings on page 132](#)
- [Managing SNMP Traps on page 131](#)

Managing SNMP Traps

Service Now users can choose to enable or disable an SNMP trap attribute to be added for a notification. To manage SNMP traps, you must have Service Now administration privileges.

To Manage SNMP traps, from the Service Now navigation tree, select **Administration > Global Settings > SNMP Configuration > Manage SNMP Traps**. The SNMP Traps Attributes page appears.

This page displays all the available trap attributes and also the notifications in which these trap attributes are sent. See [Figure 26 on page 132](#).

Figure 26: SNMP Trap Attribute Page

Administration > Global Settings > SNMP Configuration > Manage SNMP Traps

SNMP Trap Attributes	
Attribute Name	Notifications
<input type="checkbox"/> serialNumber	Service Contract Expiring, Switch over enabled for UMB, Connected Member Device Added/Removed
<input type="checkbox"/> scriptVersion	New Exposure
<input type="checkbox"/> product	New Exposure, Switch over enabled for UMB
<input type="checkbox"/> prNumber	New Exposure
<input type="checkbox"/> prLink	New Exposure
<input type="checkbox"/> platform	New Exposure, Switch over enabled for UMB
<input type="checkbox"/> partNumber	Service Contract Expiring
<input type="checkbox"/> organization	New Exposure, New Incident Detected, Case ID Assigned, Case Status Updated, New Intelligence Update, Incident Submitted, Ship-to Address Missing For Device, Connected Member Device Added/Removed
<input type="checkbox"/> lastUMBReceivedTime	Switch over enabled for UMB
<input type="checkbox"/> junosVersion	New Exposure
<input type="checkbox"/> issueDate	New Intelligence Update
<input type="checkbox"/> ipAddress	New PBN Arrival, New EOL Match, Case ID Assigned, Case Status Updated, New Incident Detected, Incident Submitted, Ship-to Address Missing For Device, Connected Member Device Added/Removed
<input checked="" type="checkbox"/> hostID	New Incident Detected, Incident Submitted, Case ID Assigned, Case Status Updated, Ship-to Address Missing For Device
<input type="checkbox"/> exposureMsg	New Exposure
<input type="checkbox"/> exposureIssueDate	New Exposure

Page 1 of 1 | Displaying 1 - 25 of 25

Submit Cancel

Notifications related to Service Insight are shown in this page only if Service Insight is enabled.

Related Documentation

- [Configuring Global Settings on page 123](#)
- [Adding an SNMP Server on page 129](#)
- [Editing and Deleting an SNMP Server on page 131](#)

Configuring Proxy Server Settings

You can configure Service Now to work with a proxy server. When you connect to a proxy server, all communication to and from JSS happens through the proxy server. Both SOCKS and HTTP proxies are supported by Service Now.

The proxy server evaluates the request according to the filters specified. For example, it may filter traffic by IP address or protocol. When the request is validated, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

To configure the proxy server settings:

1. From the Service Now taskbar, select **Administration > Global Settings > Proxy Server Configuration**.

The **Proxy Server Configuration** dialog box appears.

Figure 27: Proxy Server Configuration Dialog Box

2. Enter a valid IP address or a valid host name for the proxy server.
3. Specify the port on which the proxy server communicates with JSS.
The default port number is 1080.
4. Enter the login username for authentication.
5. Enter the password that the identified user can use to log in.
6. Click **Submit**.

The proxy server settings are saved in the Service Now database.

- Related Documentation**
- [Configuring Global Settings on page 123](#)
 - [Adding an SNMP Server on page 129](#)
 - [Editing and Deleting an SNMP Server on page 131](#)

Uploading Core Files Generated for Events

You can configure Service Now to upload core files that are generated for an event or that are related to an event (A core file is generated when there is a system problem). Core files correspond to events. You can upload specific core files either when a case is submitted for an event or after the case is opened for the event.

To upload core files:

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

The **Core File Upload Configuration** dialog box appears.

2. Select the upload preference from the **Core File Upload Preference** drop-down list.

The available options are:

- Anonymous FTP directly from device: This option enables you to upload core files directly from the router to Juniper FTP server
- Disabled-Core Files uploaded manually: This option enables you to manually upload the core files for a case
- Secure FTP upload through Service Now: This option enables you to upload core files directly from the router to Juniper SFTP server through Service Now
- Both FTP & SFTP: If this option is selected, Service Now tries to upload core files from the device to the FTP server. If this fails, then Service Now tries to upload the core files to SFTP server



NOTE: If you select this option, the credentials for FTP and SFTP servers are automatically populated.

3. Enter the required parameters in the respective fields.
4. Click **Submit**.



NOTE: For Service Now in the end-customer mode, these fields are disabled. In the end-customer mode, the values for all the fields are retrieved from the partner. The Update Credentials field will be available to update the credentials from the partner.

5. Click **Check SFTP Server** to verify the connectivity of the SFTP server.

Related Documentation

- [Organizations Overview on page 73](#)
- [Configuring Global Settings on page 123](#)
- [Administration Overview on page 71](#)
- [Updating Core File Upload Configuration on page 82](#)

Auto Submit Policy

- [Auto Submit Policy Overview on page 135](#)
- [Creating an Auto Submit Policy on page 136](#)
- [Modifying an Auto Submit Policy on page 139](#)
- [Deleting Auto Submit Policies on page 140](#)
- [Exporting an Incidents Report on page 140](#)
- [Changing the Status of Auto Submit Policies on page 141](#)
- [Changing the Status of Dampening on page 143](#)

Auto Submit Policy Overview

An auto submit policy is a policy that you create to enable Service Now to submit incidents to Juniper Support Services (JSS) automatically. While using Service Now in end-customer mode, auto submit policies allow Service Now to submit incidents automatically to the Service Now of Juniper Networks partner. When incidents are submitted to JSS, technical support cases are created with Juniper Networks and the status of the incidents are updated on the Incidents page in Service Now. When incidents are submitted automatically, they are filtered based on the JMB Filter Level setting of the Service Now organization to which the device belongs. These cases can be created from the Manage Incidents and the Create Auto Submit Policy pages.

As a Service Now customer, you can dampen incidents. Dampening prevents cases to be submitted for the same incident if the incident occurs within a configurable time period called dampening period. Dampening policy is assigned to individual events. This is applicable to duplicate incidents (same errors, error messages and devices) if Auto Submit Policy is activated. You can select a dampening period for which alerts are dampened for the same incidents and for the same device(s), device Group or organization.

Service Now uses the event ID and synopsis on the incident to dampen an incident. Whenever an event occurs on a device, Service Now checks if an auto submit policy is defined for that device. If an auto submit policy is defined, Service Now checks for the dampening status on the policy. If the dampening status is enabled, Service Now gets the user defined dampening interval for the event reported on a device. If a dampening interval is found, Service Now checks when the last incident was created for an event ID and synopsis. If the last incident occurred before the defined dampening interval or if it had occurred during the defined dampening interval but is in closed state, a new incident is created; otherwise incident is not created. Event RMA is always dampened.

To view auto submit policies, select **Administration > Auto Submit Policy**, from the Service Now taskbar. The Auto Submit Policy page appears as shown in [Figure 28 on page 135](#).

Figure 28: Auto Submit Policy Page

Name	Status	Events	Devices	Incidents Submitted	Dampening	Date Created	Last Modified
ASP	Disabled	3	2	0	Enabled	Oct 3, 2013 4:48:34 PM IST	Oct 4, 2013 3:25:38 PM IST

You can perform the following tasks from the View Auto Submit Policy page

- Change the status of auto submit policies
- Export incidents report
- Delete auto submit policies

- Modify an auto submit policy
- Change dampening status

Related Documentation

- [Modifying Auto Submit Policy on page 106](#)
- [Creating an Auto Submit Policy on page 136](#)
- [Adding an SNMP Server on page 129](#)
- [Creating and Editing a Notification Policy on page 187](#)

Creating an Auto Submit Policy

An auto submit policy enables incidents that occur on devices to be submitted to JSS automatically, creating a Tech Support Case. Although events with priority P1 can be included in auto submit policies, they do not get automatically submitted to JSS. Therefore, P1 events must be submitted manually and JTAC should be called immediately.

To create an auto submit policy:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy > Create Auto Submit Policy**.

The Choose devices to include in Auto Submit Policy page appears as shown in [Figure 29 on page 136](#).

Figure 29: Auto Submit Policy Creation Page

Administration > Auto Submit Policy > Create Auto Submit Policy

Choose devices to include in Auto Submit Policy

Policy Name:

Show:

[Show Selected Devices](#)

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle	Policy
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device1	33108	M10I	11.4R7.5	3.7R1.2	
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device2	PV0213250012	ACX1100	12.3X51-D10.5	3.7R1.2	ASP
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device3	NK0212350232	ACX2100	12.3X52-D10.4		
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device4	JN11B7992AEA	M120	11.4R7.5	3.7R1.2	ASP
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device5	E4008	MX80-48T	11.4R6-S2		
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device6	73682	M40E	11.4R7.5		
<input type="checkbox"/> JCare-Plus	Default for JCare-Plus	device7	AB3510AA0021	SRX3600	11.4R9.4		

Page 1 of 1 | [Next](#) [Cancel](#)

Displaying 1 - 7 of 7

2. In the **Policy Name** field, enter a name for the policy. The name can contain only alphanumeric (a-z, A-Z, 0-9), underscores (_), and hyphens (-). The maximum number of characters allowed is 255.
3. Select the devices for which you want to create an auto submit policy.
 - To filter devices by their organization, in the **show** list, select **By Device Group** and select an *Organization* in the **Organization** field. A new list displays devices filtered organizations or device groups

- To filter devices by device group, in the **show** list, select **By Device Group** and select a *Device Group* from the **Device Group** field. A new list displays devices filtered organizations or device groups

A list is displayed by filtering the devices based on the selected organization or device group.

- Select the devices for which you want to assign an auto submit policy.

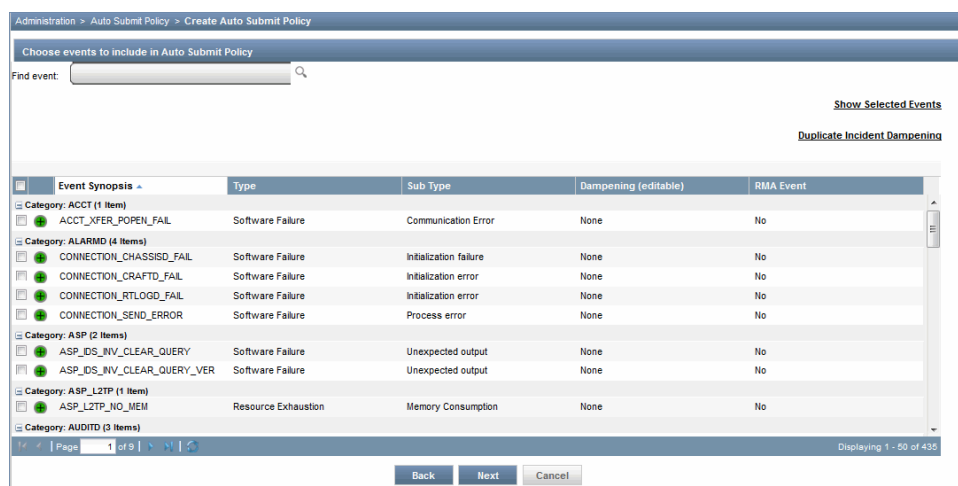
(Optional) To display the list of selected devices to which you want to assign the auto submit policy:

- Click the **Show Selected Devices** link.
The **Selected Devices** dialog box displays the list of devices that you selected.
- Verify the list and click **Close** to return to the previous page.

- Click **Next**.

The **Choose events to include in Auto Submit Policy** page appears.

Figure 30: Choose Events to Include in Auto Submit Policy Page





- Select the events that you want to include in the auto submit policy. Events with priority P1 are not available for selection. Do not include events that are inactive for the selected devices. You can easily identify these events by looking at the icons that are used to represent them (see [Table 17 on page 137](#)).

To find events, type the event name in the **Find event** field and then select the event. As you type an event name, all the events with names beginning with the text that you entered are displayed in the list. For example, as shown in [Figure 30 on page 137](#), when you type **audi** in the **Find event** field, all events with names beginning with audi are listed.

Table 17: Icons That Represent the Event Types and Their Descriptions

Event Icons	Descriptions
	Event is inactive for all the selected devices. Do not include this event in the auto submit policy.

Table 17: Icons That Represent the Event Types and Their Descriptions (*continued*)

Event Icons	Descriptions
	Event is inactive for some of the selected devices.
	Event is active for all the selected devices.
P1	Event is, by default, priority P1 for one or more selected devices. Although these events can be included in the auto submit policies, they do not get automatically submitted to JSS. You can open a case for these events only by contacting JSS directly over phone.

7. (Optional) To display the list of selected events that you want to include in the auto submit policy:
 - a. Click the **Show Selected Events** link.
The **Selected Events** dialog box displays the events that you selected.
 - b. Verify the list and click **Close** to return to the Choose events to include in Auto Submit Policy page.
8. Click the **Duplicate Incident Dampening** link to set the dampening interval for the selected events. The Duplicate Incident Dampening dialog box appears.
9. Choose a dampening interval from the **Dampen Incidents for** drop-down list.
 - None creates an incident in Service Now for each occurrence of the selected events on the selected devices.
 - Always: After the first occurrence of the selected events on the selected devices, no incident is created for the events in Service Now. An incident is created on the first occurrence of the event. No incident is created for a selected event on a selected device until the incident is closed or deleted.

Always does not create incidents after the first occurrence of the selected events on the selected devices. An incident is created for the first occurrence of the selected events on the selected devices. The next incident is created only after the existing incident for the event is closed or deleted.
 - Dampening intervals of 1hr, 2hr, 3hr, etc. does not create incidents in Service Now for the specified time duration after the first occurrence of a selected event in a selected device.
10. Click **Next**.
The Submit Case Options page appears.
11. Click the **Enter Email Id** field to enter an e-mail IDs in the format user@example.com.
To add, or delete multiple e-mail IDs, use the **Add Email** and **Delete** buttons.
12. Click **Modify** to modify the site ID or username details of organization.
The Make Selection to Change Site ID or Use dialog box appears.
 - To modify the site ID, click **Default Org**, and select the site ID from the **Site ID** list.

- To modify the user name, click **User Name** , and enter the username and password of the selected Site ID or organization in their respective fields. After your user credentials are validated, click **Get Sites** to select a site ID specific to the new user.

13. Click **OK**.

The Summary of Auto Case Policy to be created page lists the details such as the selected events, the devices on which they occurred, the event synopsis, and the dampening status.

The Submit Case Options page appears again.

14. Select the **Upload Core Files** check box if you want the auto submit policy to upload core files to service for the selected events.
15. , Select the **Delete Core Files from Router after Uploading** check box If you want to delete core files from the device after uploading it to Service Now.
16. In the **Follow Up Method** list, select the method that you would like to use to follow up on the case . The available options are Email Full Text Update, Email Secure Web Link, and Phone Call.
17. In the **Priority** field, select the priority of the case. The available options are Critical, High, Medium, and Low. The default priority is Low.
18. In the **Add Comments to Synopsis** and **Add Comments to Description** fields, enter a synopsis and description for the case.

When submitting on-demand or off-box incidents, you can edit the auto-generated synopsis and description. The maximum number of characters allowed for the synopsis and the description are 255 and 1,028 respectively.

19. Click **OK**.

The auto submit policy is created and listed in the View Auto Submit Policy page. When the selected events occur on the devices with auto submit policy, incidents are automatically submitted to Juniper Support Services (JSS) and a Tech Support Case is created.

By default, auto submit policies are enabled. To disable auto submit policies, see [“Changing the Status of Auto Submit Policies” on page 141](#).

Related Documentation

- [Adding an SNMP Server on page 129](#)
- [Creating and Editing a Notification Policy on page 187](#)
- [Administration Overview on page 71](#)
- [Modifying Auto Submit Policy on page 106](#)

Modifying an Auto Submit Policy

Junos Space enables you to modify the events and devices that are specified in an auto submit policy.

To modify an auto submit policy:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**.
The Auto Submit Policy page appears.
2. Select the auto submit policy that you want to modify and select **Modify Auto Submit Policy** from either the **Actions** list or the right-click menu.

The details of the selected auto submit policy are displayed in an editable format.
3. Make your modifications to the events and devices for which the incidents must be automatically submitted to JSS.
4. Click **Save**.
Your changes are saved and the auto submit policy is listed in the Auto Submit Policy page with your modifications.

**Related
Documentation**

- [Adding an SNMP Server on page 129](#)
- [Creating and Editing a Notification Policy on page 187](#)
- [Modifying Auto Submit Policy on page 106](#)

Deleting Auto Submit Policies

To delete auto submit policies:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**.
The Auto Submit Policy page appears.
2. Select the auto submit policies that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.

The Delete Policies dialog box appears.
3. Click **Delete** to confirm.

The selected auto submit policies are deleted and removed from the View Auto Submit Policy page.

**Related
Documentation**

- [Auto Submit Policy Overview on page 135](#)
- [Creating an Auto Submit Policy on page 136](#)
- [Modifying an Auto Submit Policy on page 139](#)
- [Adding an SNMP Server on page 129](#)
- [Creating and Editing a Notification Policy on page 187](#)

Exporting an Incidents Report

To export information about incidents stored in auto submit policies:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**.
The Auto Submit Policy page appears.

2. Select the auto submit policies that you want to export to an Excel file, and click **Export Incidents Report** from either the **Actions** list or the right-click menu.

The Export Incidents Report dialog box is displayed.

3. Click the **Click here to download Incidents for Auto submit Policy above** link to generate the Excel file.
 - To open the Excel file, select **Open with** and click **Open**.
 - To save the Excel file on your local file system, select **Save File**, navigate to the folder where you want to save the Excel file, and click **OK**.
Detailed information about the selected auto submit policies appears in an Excel spread sheet.

Related Documentation

- [Modifying an Auto Submit Policy on page 139](#)
- [Adding an SNMP Server on page 129](#)
- [Creating and Editing a Notification Policy on page 187](#)

Changing the Status of Auto Submit Policies

Incidents can be submitted to JSS only when an auto submit policy is enabled. To enable or disable an auto submit policy:

To change the status of auto submit policies:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**.
The Auto Submit Policy page appears.
2. Select the auto submit policies for which status need to be enabled and select **Change Status** from either the **Actions** list or the right-click menu.

The **Change Auto Submit Policy Status** dialog box displays the current status of the selected auto submit policies. See [Figure 31 on page 142](#).

Figure 31: Change Auto Submit Policy Status Page

Change Auto Submit Policy Status

Confirm status change for below items:

Policy Name	Current Status
ASP	Disabled

☐ Schedule at a later time

Change Status Cancel

(Optional) Click the **Schedule at a later time** check box and specify a date and time to enable the auto submit policy.

3. Click **Change Status**.

The action is initiated and a Jobs dialog box displays the Job ID. Click the link to view the Jobs page where you can view the status of this action.

4. After the job is complete, click **OK**.

The Quick View of the auto submit policy is displayed in the Auto Submit Policy page.

[Table 18 on page 142](#).

Table 18: Auto Submit Policy Icons

Icon	Description
	The auto submit policy is disabled.
	The auto submit policy is enabled.

Related Documentation

- [Modifying an Auto Submit Policy on page 139](#)
- [Adding an SNMP Server on page 129](#)
- [Auto Submit Policy Overview on page 135](#)
- [Creating an Auto Submit Policy on page 136](#)
- [Creating and Editing a Notification Policy on page 187](#)
- [Changing the Status of Dampening on page 143](#)

Changing the Status of Dampening

The Change dampening status on View Auto Submit Policy page enables you to change the dampening status for an auto submit policy. You can select one or multiple auto submit policies and change their dampening status (from Enabled to Disabled or vice versa).

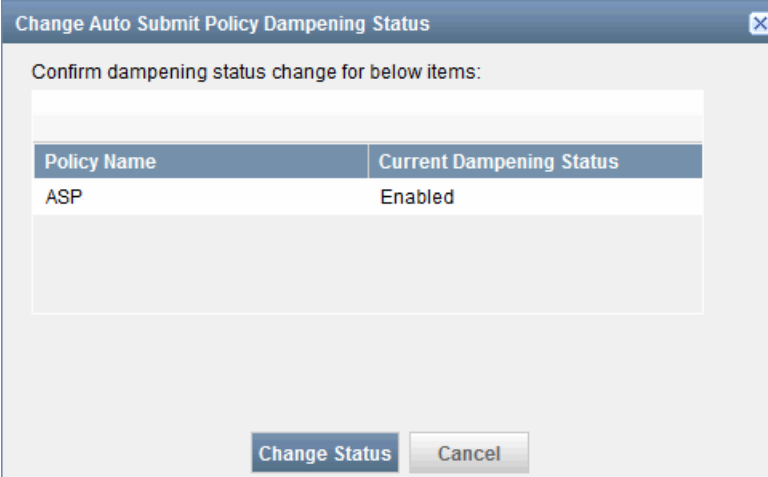
The incidents are dampened only if the dampening status of a policy is enabled.

To change the dampening status:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**. The Auto Submit Policy page appears
2. Select the auto submit policies whose dampening status needs to be changed.
3. Select **Change dampening status** from either the **Actions** list or the right-click menu.

The Change Auto Submit Policy Dampening Status dialog box appears showing the selected Auto submit policies. See [Figure 32 on page 143](#).

Figure 32: Change Auto Submit Policy Dampening Status Page



Policy Name	Current Dampening Status
ASP	Enabled

4. Click **Change Status**. The dampening status of the policy is changed.

Related Documentation

- [Modifying an Auto Submit Policy on page 139](#)
- [Adding an SNMP Server on page 129](#)
- [Auto Submit Policy Overview on page 135](#)
- [Creating an Auto Submit Policy on page 136](#)
- [Creating and Editing a Notification Policy on page 187](#)
- [Changing the Status of Auto Submit Policies on page 141](#)

Address Group

- [Address Group Overview on page 144](#)
- [Creating Address Group on page 145](#)
- [Modifying Address Group on page 145](#)
- [Deleting Address Group on page 146](#)
- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)
- [Associating Devices with an Address Group From an Organization ILP on page 148](#)
- [Associating Devices with an Address Group from a Device Group ILP on page 149](#)
- [Associating Devices with an Address Group From a Service Now Devices ILP on page 150](#)

Address Group Overview

Using Service Now, a client can associate address location to devices, and a user can associate a device location or a ship-to-address to a device. The ship-to-address is used by service now to inform the logistics team of Juniper where to ship a particular part in case an RMA case is opened.

Partner proxy users can use the partner address instead of customer address when submitting cases to Juniper. This can be done through a setting at the connected member and when submitting a case manually. For an auto submit case policy, the partner address can be used if this feature is selected by the partner. Otherwise the end-customer address must be used. If the partner uses the partner address, both partner address and customer address must be shown for the device. However, only the partner address is shown when submitting an incident to Juniper.

Service Now also provides the functionality wherein a client can update notes to an already opened CRM case with juniper.

In Service Now, a set of already defined address groups are listed in the View Address Group page. The tabular view of the View address Group pages provides details about the address group and the devices.

You can perform the following tasks from the View Address Group page:

- Create a new address group
- Modify an existing address group
- Delete an address group
- Associate address group to a set of devices

A user has the option to associate devices to any of the address groups defined in the system. Devices can also be associated to an address group subtypes (Location, Ship-to, and Both) from the organization ILP, device group ILP, and devices ILP. A user can choose to associate address group on the corresponding ILP.

Related Documentation

- [Creating Address Group on page 145](#)

- [Modifying Address Group on page 145](#)
- [Deleting Address Group on page 146](#)
- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)

Creating Address Group

To create an address group:

1. From the Service Now navigation tree, select **Administration** > **Create Address Group**. The Create Address Group page appears.
2. Enter data in the relevant fields.

The Address Group name must be unique and can contain alphanumeric character, space, hyphen, and underscore. The maximum number of characters allowed is 255.
3. Select **Submit**.

The new address group is created and displayed on the Address Group page.

Related Documentation

- [Address Group Overview on page 144](#)
- [Modifying Address Group on page 145](#)
- [Deleting Address Group on page 146](#)
- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)

Modifying Address Group

To modify an address group:

1. From the Service Now navigation tree, select **Administration** > **Address Group**. The Address Group page appears.
2. Select the address group that you need to modify, and select **Modify Address Group** from either the **Actions** list or the right-click menu. The Modify Address Group page appears.
3. Modify the relevant fields.



NOTE: You cannot modify an address group name on this screen.

4. Select **Submit**.

The address group is modified and can be viewed on the Address Group page.

Related Documentation

- [Address Group Overview on page 144](#)
- [Creating Address Group on page 145](#)
- [Deleting Address Group on page 146](#)

- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)

Deleting Address Group

To delete an address group:

1. From the Service Now navigation tree, select **Administration** > **Address Group**. The Address Group page appears.
2. Select the address groups that you need to delete, and select **Delete** from either the **Actions** list or the right-click menu.

The Delete Address Groups page appears.

3. Click **Delete** to delete the selected address groups.

The selected address groups are deleted and no longer listed on the Address Group page.

Related Documentation

- [Address Group Overview on page 144](#)
- [Creating Address Group on page 145](#)
- [Modifying Address Group on page 145](#)
- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)

Associating Devices with an Address Group From an Address Group ILP

Using Service Now, you can associate devices with address groups from an address group ILP.

To associate a device with an address group from address group ILP:

1. From the Service Now navigation tree, select **Administration** > **Address Group**.
The Address Group page appears.
2. Select the address group that needs to be associated with a device, and select **Associate Devices** from either the **Actions** list or the right-click menu. The Associate Address Group to Devices page appears. See [Figure 33 on page 147](#).

Figure 33: Associate Address Group to Devices Page

Associate Address Group to Devices

Name: test
Address:
City: t
State: t
Country: t
Zip: t

Select Address Types

Location
Ship-to
Both

Associate or remove devices from Location

Hostname	Platform	Serial Number	Organization	Device Group
ex-2200-sn3	junos-ex	CW0210403356	ec	Device Group for ec
sn-space-ex4500-sys1	junos-ex	GG0213130986	ec	Device Group for ec
ex-4200-an1	junos-ex	BM0210329678	ec	Device Group for ec
ex-8200-sn1	junos-ex	CA1710431095	ec	Device Group for ec
ex-4200-an4	junos-ex	BM0210329621	ec	Device Group for ec

Page 1 of 1 | Showing 1 - 7 of 7 | Show 30 | It's

Close

You can associate devices to this address group in any of the following sub types: Location, Ship-to or Both. These subtypes of the address group represent the device location or ship-to address of a device. In case of an RMA event, the ship-to address is used by logistics team of Juniper to ship the defective part to the customer directly, without manual intervention. A device can have only one location or ship-to address associated to it. You can click **Location** to associate a device to a location. Repeat the same procedure for Ship-to and Both. Clicking on the left hand side menu alone results in displaying the already associated devices for this subtype. If you associate a device to both Ship-to and Location on an address group, all the previous associated links to the device are removed and the latest changes are effective.

You can assign an address to a device as its location, ship-to or both. In case of an RMA event, the ship-to address is used by the logistics team of Juniper to ship the defective parts for the device. A device can have only one location and ship-to address.

- The address group must be assigned to the devices as the address of their location, shipping address or the address for both the location and shipping.
 - To assign the address group as the address of a device location, under **Select Address Types**, click **Location**.
 - To assign the address group as the shipping address for a device, under **Select Address Types**, click **Ship-to**.
 - To assign the address group as the address for both shipping and location, under **Select Address Types**, click **Both**.
- In the **Associate or remove devices from** section, click the Plus icon.

The Select Devices page appears listing all the devices present in service now. If required, filter the devices.

- To filter by organization, in the **Show** list, select By Organization and select the Organization from the **Organization** list.

- To filter by Device Group, in the **Show** list, select By Device Group and select the Device Group from the **Device Group** list
 - To filter by name of device, in the search field, enter the first few characters of the device name
5. Select the devices from the device list to assign the address group and click **Submit**. The address group is assigned as the address of the selected devices' location, shipping address or the address for both shipping and location as specified in Step 3 and the Associate Address Group to Devices page is displayed.
 6. To remove a device association from one of the subtypes, click on the subtype link on the left. The devices associated to the selected sub type will be listed. Select a list of devices on the right and then click on the cross button on the right.
 7. The Disassociate Devices window appears. Click **Remove**. The devices are removed from this address group subtype (Location, Ship-to or Both).

Devices can also be associated to an address group sub types through organization ILP, device group ILP and devices ILP.

**Related
Documentation**

- [Address Group Overview on page 144](#)
- [Creating Address Group on page 145](#)
- [Modifying Address Group on page 145](#)
- [Deleting Address Group on page 146](#)

Associating Devices with an Address Group From an Organization ILP

Using Service Now, you can associate devices to address groups from organization ILP.

To associate a device to an address group from organization ILP:

1. From the Service Now navigation tree, select **Administration > Organizations**.
The Organizations page appears.
2. Select the address group that needs to be associated with a device, and select **Associate Address Group** from either the **Actions** list or the right-click menu.

The Associate Devices to Address Group page appears.

Figure 34: Associate Devices to Address Group Page

<input type="checkbox"/>	Hostname	Serial Number	Location	Ship-To
<input checked="" type="checkbox"/>	device1	JN11B7992AEA		
<input checked="" type="checkbox"/>	device2	NK0212350232		
<input checked="" type="checkbox"/>	device3	AB3510AA0021		
<input checked="" type="checkbox"/>	device4	E4008		
<input checked="" type="checkbox"/>	device5	LX0213052164		

3. Select the address group/Address group subtype [i.e. Location and Ship to Address] from the combo box and click **Submit**.

All the selected devices are associated to the new address group/address subtype. This page lists the devices present under the selected organization. The Location and Ship-to Address fields show address group names if the devices already have an association present in the system

- Related Documentation**
- [Organizations Overview on page 73](#)
 - [Associating Devices with an Address Group From an Address Group ILP on page 146](#)

Associating Devices with an Address Group from a Device Group ILP

Using Service Now, you can associate devices to address groups from device group ILP.

To associate a device to an address group from device group ILP:

1. From the Service Now taskbar, select **Administration** > **Device Groups**. The Device Groups page appears.
2. Select the device that needs to be associated with an address group, and select **Associate Address Group** from either **Actions** or the right-click menu.

The Associate Devices to Address Group page appears. This page lists the devices present under this selected device group. The Location and Ship-to Address fields will show address group names if the devices already have an association present in the system. See [Figure 35 on page 150](#).

Figure 35: Associate Devices to Address Group Page

	Hostname	Serial Number	Location	Ship-To
<input checked="" type="checkbox"/>	device1	JN11B7992AEA		
<input checked="" type="checkbox"/>	device2	NK0212350232		
<input checked="" type="checkbox"/>	device3	AB3510AA0021		
<input checked="" type="checkbox"/>	device4	E4008		

3. Select the devices in the device group to be associated with the address group.
Selecting the check box to the left of **Hostname** selects all the devices.
4. In the **Location** and **Ship-to Address** fields, select the location and ship-to address of the devices.
5. Click **Submit**.
All the selected devices will get associated to the new address group and address type.

Related Documentation

- [Device Groups Overview on page 83](#)
- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)
- [Associating Devices with an Address Group From an Organization ILP on page 148](#)
- [Associating Devices with an Address Group From a Service Now Devices ILP on page 150](#)

Associating Devices with an Address Group From a Service Now Devices ILP

Using Service Now, you can associate devices to address groups from devices ILP.

To associate a device to an address group from devices ILP:

1. From the Service Now taskbar, select **Administration > Service Now Devices**. The Service Now Devices page appears.
2. Select the device needs to be associated with an address group, and select **Associate Address Groups** from either **Actions** or the right-click menu.

The Associate Devices to Address Group page appears. This page lists the devices present under this selected device group. The Location and Ship-to Address fields will show address group names if the devices already have an association present in the system.

3. In the **Location** and **Ship-to Address** fields, select the location and ship-to address of the devices.

4. Click **Submit**.

All the selected devices will get associated to the new address group and address type.

**Related
Documentation**

- [Service Now Devices Overview on page 86](#)
- [Associating Devices with an Address Group From an Address Group ILP on page 146](#)
- [Associating Devices with an Address Group From an Organization ILP on page 148](#)
- [Associating Devices with an Address Group from a Device Group ILP on page 149](#)

E-mail Templates

- [E-mail Templates Overview on page 152](#)
- [Viewing E-mail Templates on page 153](#)
- [Modifying E-mail Templates on page 153](#)

E-mail Templates Overview

You can use Service Now to send notification for an event through e-mail. Service Now has default e-mail templates whose contents can be modified. However, you cannot modify or delete the default template files. As an administrator, you can update or configure the e-mail content sent to the users during notification.

E-mail templates provide the format for sending e-mail notifications for events to users. There is a default E-mail template for various situations such as for sending notifications listing the devices for which technical support contract licenses are to be expired in 60 days or for sending notifications listing the devices that are sending device snapshots.

These templates can be modified. Service Now provides default E-mail templates for which cannot be deleted or modified.

Service Now displays two types of templates: license specific and generic e-mail templates. The display of templates is based on the installation of service now. If Service Now is installed in standalone mode, only standalone related templates are displayed. If Service Now is installed in partner mode only partner related templates are displayed.

Figure 36: E-mail Templates Page

Administration > Email Templates				
Actions		0 Item Selected		
<input type="checkbox"/>	Name	Description	Created By	Last Updated
<input type="checkbox"/>	Connected member device added/removed	This template is used by Service Now for sending email notificati...	super	Oct 4, 2013 1:30:43 PM IST
<input type="checkbox"/>	Contract Expiry Info Received	This template is used by Service Now when sending email notificat...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	Devices Not Sending Device Snapshot	This template is used by Service Now for sending email notificati...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	End Customer Case Closed in Partner Proxy	This email is sent when an end customer case (from a Service Now ...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	End Customer Case Created in Partner Proxy	This email is sent when an end customer case (from a Service Now ...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	End Customer Case Updated in Partner Proxy	This email is sent when an end customer case (from a Service Now ...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	End Customer Incident Submitted to Partner Proxy	This email is sent when an case is submitted to the Service Now P...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	Incident Flagged to Users	This template is used by Service Now for sending email notificati...	Service Now	Jul 30, 2013 12:52:03 PM IST
<input type="checkbox"/>	Incident Submitted to Juniper by Partner Proxy	This template is used by Service Now for sending email notificati...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	Incomplete RMA Incident Submitted to Juniper	This template is used by Service Now for sending email notificati...	Service Now	Jul 30, 2013 12:52:02 PM IST
<input type="checkbox"/>	Juniper Technical Support Case Created for Incident from Partner Proxy	This template is used by Service Now for sending email notificati...	Service Now	Jul 30, 2013 12:52:03 PM IST
<input type="checkbox"/>	Juniper Technical Support Case	This template is used by Service Now	Service Now	Jul 30, 2013 12:52:03 PM

From the e-mail templates page in Service Now, you can perform the following tasks:

- View e-mail templates
- Modify e-mail templates

Related Documentation

- [Viewing E-mail Templates on page 153](#)
- [Modifying E-mail Templates on page 153](#)

Viewing E-mail Templates

The E-mail templates page in Service Now helps you manage e-mail templates.

To view e-mail templates:

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

The E-mail Templates page appears.

2. Double click the required template from the list.

The Email Template Details page appears. The Email Template Details page includes the following information:

- Name of the incident
- Date and time when the template content was last updated
- Description of the template
- Subject of the e-mail template
- Template contents that can be modified

Related Documentation

- [E-mail Templates Overview on page 152](#)
- [Modifying E-mail Templates on page 153](#)

Modifying E-mail Templates

Using Service Now, you can modify the contents of the e-mail templates. An e-mail template for an End customer contains \$ variables and static content. \$ variables cannot be modified but can be removed. All other static content can be modified on a template.

To modify an e-mail template:

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

The Email Templates page appears.

2. Select the e-mail template whose content you want to modify and select **Modify** from either the **Actions** list or the right-click menu.

If a template contains HTML table, then the Template contents field is followed by table columns in a grid separately. You can remove a column from the template by clearing the check box for that column. The column can be added again by selecting it again.

Related Documentation

- [E-mail Templates Overview on page 152](#)
- [Viewing E-mail Templates on page 153](#)

CHAPTER 7

Service Central

- [Service Central Overview on page 155](#)
- [Incidents on page 157](#)
- [Information on page 174](#)
- [JMB Errors on page 184](#)
- [Notifications on page 186](#)

Service Central Overview

The Service Central workspace enables you to manage incidents, information messages, device snapshots, notifications, and error JMBs. Incidents are problem events that are detected in a device and sent to the Service Now application. When an event occurs on a device, AI-Scripts installed on the device create files called Juniper Message Bundles (JMBs) that contain comprehensive information about the device identity, the problem event, and diagnostics. The JMB file is then transferred securely from the device to Service Now. Service Now searches for new incidents and displays the incidents on the Incidents page within Service Central.

The Service Central workspace provides the following three gadgets:

- Incident severities—provides a graphical representation of the incidents generated and their severity.
- Incident priorities—provides a graphical representation of the incidents generated and their severity.
- My Incidents—provides a graphical representation of the incidents created new, flagged to you, or owned and changed by you.

Clicking the bar on the graph takes you to the respective incidents.

Figure 37: Service Central Gadgets



After viewing an incident, you can use the Incidents menu on the Service Now navigation tree to submit a case to the Juniper Support Systems (JSS). You can also notify other users about the incident, assign a user as an owner of the incident, and delete the incident from the device.

In addition to reporting incidents, AI-Scripts also send device information regularly to Service Now in the form of Information Juniper Message Bundles (iJMBs). The iJMBs are then processed and displayed on the Device Snapshots page. You can upload these iJMBs to JSS, where they are processed and analyzed to provide preventive analysis and alerts. You can view the content of these iJMBs and export them to HTML format.

In certain cases, when devices stop sending device information, Service Now generates the iJMBs for all the devices associated to a device group. These iJMBs are generated based on the commands available in directive file pre-loaded in Service Now. The content of these iJMBs is the same as AI-Scripts generated iJMBs. Service Now administrator receives a message when Service Now generates iJMBs automatically for one or more devices.

A JMB is considered erroneous if it does not comply with the standard data structure that Service Now requires or if it contains data elements that Service Now does not accept. Service Now identifies these JMBs and displays them on the JMB Errors page from where they can be viewed and downloaded.

You can use a notification policy to specify the events for which you want to receive a notification. The options are New Incident Detected, Case Submitted, Case Status Updated, and Intelligence Update Received. Notification policies define other characteristics (filters) that you can use to fine tune the conditions under which you

receive a notification. You can even define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

Some tasks within the Service Central workspace, such as assigning messages to a connected member and updating an end-customer case, are enabled only when Service Now operates in the end-customer mode. For more information about the Service Now modes, see [“Service Now Modes” on page 42](#).

The Service Central page graphically displays information about the severity and priority of incidents and the incidents you created.

Using Service Central, you can perform the following tasks:

- Assign a user to own and manage incidents, notify users about the incidents, update the status of the incidents, and delete incidents.
- View and delete iJMBs, and export device data to HTML format.
- Assign messages to end-customers (enabled if Service Now is operating in the partner-proxy mode).
- Update customer cases (enabled if Service Now is operating in the partner-proxy mode).
- View, download, and delete JMBs with errors.
- View Knowledge Base articles associated with incidents.
- View information about devices that are susceptible to known issues.
- Generate JMBs on demand.
- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

**Related
Documentation**

- [Service Now Overview on page 34](#)
- [Service Now Modes on page 42](#)
- [Incidents Overview on page 158](#)
- [Device Snapshots Overview on page 180](#)
- [Messages Overview on page 175](#)
- [JMBs with Errors on page 184](#)
- [Notification Policies Overview on page 186](#)

Incidents

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)

- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Deleting an Incident on page 164](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)
- [Uploading Core Files for Incidents on page 174](#)

Incidents Overview

An incident is the occurrence of a defined event in a device. When an incident, such as a process crash, an application-specific integrated circuit (ASIC) error, or a fan failure occurs on an AI-Scripts-enabled device, the AI-Scripts builds a Juniper Message Bundles (JMBs) file with the incident data which is accessed by Service Now.

A JMB file is an XML file that contains diagnostic information about the device and other information specific to the condition that triggered the incident. The incident contains information such as hostname, time stamp of the incident, synopsis, description, chassis serial number of the device, and the severity and priority of the incident.

These JMB files are securely transferred from the device to the Service Now application. After a JMB is generated, it is stored at a defined location in the device from where Service Now accesses it and display it in the Incidents page.

Service Now uses Device Management Interface (DMI), which is an extension to the NETCONF network management protocol, to access JMBs from devices. The Incidents page provides a user interface to view incidents chronologically, by organization name, and by device group. The Quick view of this page helps you differentiate incidents with various icons. These icons indicate incident priority levels and also whether the incidents are submitted to JSS. See *Service Now Icons and Inventory Pages*.

From the Incidents workspace, you can navigate to the **View Tech Support Cases** and **View End-Customer Cases** pages. The **View Tech Support Cases** page displays the technical support cases that you can open with JSS. You can open these cases only after you create an organization and the organization's site ID is validated. Site IDs denote the customer identity used in the Juniper Technical Assistance Center (JTAC) Clarify trouble ticketing system.

To stay updated of the events that occur in Service Now, you can create notification policies that instantly notify you of an event in the form of e-mails or SNMP traps.

The incidents are displayed in a table as follows: You can select the parameters to display and sort them in the ascending or descending order.

- Incident ID
- Organization

- Device group
- Defect type
- Platform type
- Incident type

**NOTE:**

- The incident type Event-RMA indicates that an RMA event is detected on the Service Now managed devices.
- The incident type Event (low end) indicates that the JMB generated on a device is a low impact JMB. User can manually collect troubleshooting data and update case through Case Manager or Service Now.
- The incident type Request RMA indicates that an RMA incident is detected on Service Now managed devices.

- Time of occurrence
- Owner
- Submission status
- Incidents that are flagged to you

You can perform the following tasks from the Incidents page:

- Submit an incident to create a JTAC case
- Flag the incident to another user
- Assign the incident to another user
- Delete an incident
- View the details of a Juniper Message Bundle (JMB)
- View a Knowledge Base (KB) article pertaining to the incident
- View a case in the Juniper Networks Case Manager
- Remove a flag from the incident
- Add an e-mail address to the mailing list of an incident
- View technical support cases
- Upload core files



NOTE: Junos OS devices may not provide specific time zones for incidents, and hence Service Now may display an incorrect time of occurrence for incidents. For example, when the time zone is EST, Service Now uses US EST by default, while the time zone can also be AEST (Australian EST).

Related Documentation

- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Assigning an Incident Owner

You can assign a user to own and manage an incident. The owner tracks the progress of the related case and the updates from JSS.

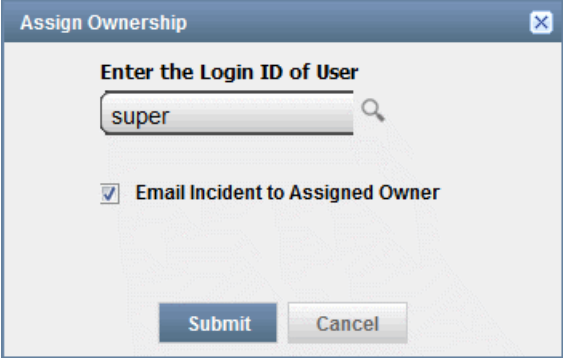
To assign an incident to a Service Now user:

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

The Incidents page appears.

2. Select the incident to which you want to assign an owner, and select **Assign Ownership** from either the **Actions** list or the right-click menu.

The **Assign Ownership** dialog box appears.

The image shows a web-based dialog box titled "Assign Ownership" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Enter the Login ID of User" with a text input field containing the word "super" and a search icon (magnifying glass) to its right. Below this, there is a checked checkbox labeled "Email Incident to Assigned Owner". At the bottom of the dialog, there are two buttons: "Submit" and "Cancel".

3. Enter the login ID of the user to whom you want to assign the incident.
If required, click the search icon to display the list of available users.
4. Select the **Email Incident to Assigned Owner** check box to send an e-mail notification to the assigned owners of the incident. This option is selected by default.
5. Click **Submit**.

The incident is assigned to the specified user. See [“Viewing Device Snapshot Details” on page 182](#).

Related Documentation

- [Incidents Overview on page 158](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Flagging an Incident to a User

You can flag an incident to a user who might be affected by the incident or needs to be aware of updates to it. When changes are made to this incident, the user receives an e-mail. If an incident is flagged to you, the Flag column of that incident in the Incidents table displays **Yes**; If not, it displays **No**.

To flag an incident to a user:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents table appears.
2. Select the incident that you want to flag to a user, and select **Flag to Users** from either the **Actions** list or the right-click menu.
The **Flag to Users** dialog box appears and displays the names of Service Now users.
3. Select the user or users to whom you want to flag the incident.
4. Select the **Email Incident to Flagged Users** check box to send an e-mail notification to all the flagged users.
This option is selected by default.
5. Click **Submit**. The incident is flagged to the selected users.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Deleting an Incident on page 164](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Checking Incident Status Updates on page 162](#)

- [Exporting Incident Data on page 163](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Checking Incident Status Updates

In Service Now, incidents are the occurrence of a predefined problem in a device. Information about these incidents is sent to the Service Now application. Service Now routinely checks for new incidents. The **Manage Incidents** page displays the incidents chronologically by organization name and device group.

You can use the Incidents page to submit an incident to JSS for creating a case. The submission status of the incident appears in the Status column on the Incidents page. After you submit the incidents, the status is **Submitted**. When JSS creates the case, the status changes to **Created** and the Case ID appears. Further updates to the incident change the incident's status to **Updated**.

Service Now provides three ways to check incident status.

- Using Junos Space logs. The Junos Space log of an incident displays a list of the status changes.
- Using notification policies. You can create a notification policy to notify users whenever the status of an incident is updated. For more information about creating notification policies, see ["Creating and Editing a Notification Policy" on page 187](#).
- Using the Service Central page. The My Incidents graph on the Service Central page displays the number of incidents whose status has changed since you last logged in. It also displays other information such as the number of incidents that were flagged to you, the number of incidents that you own, and the number of new incidents that were added since your last logged in.

To view the Service Central page, select **Service Central** from the Service Now navigation tree.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Deleting an Incident on page 164](#)
- [Exporting Incident Data on page 163](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)

- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Exporting Incident Data

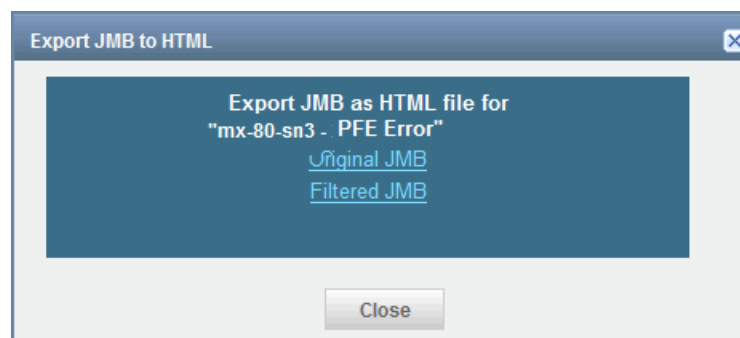
You can export JMB data along with its attachments as HTML files and save them on your local file system. A JMB is exported as a zipped folder. Logs are not exported. The view of the exported JMB file is the same as that when viewed on the View JMB page in Service Now. However, the option to download the attachments and log files is not available in an exported JMB file.

To export incident data in HTML format:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. On the Incidents page, select the incident whose details you want to export.
3. From the Actions menu, select **Export JMB to HTML**. Alternatively, right-click an incident and select **Export JMB to HTML**.

The Export JMB to HTML dialog box displays links to the original and filtered JMBs, as shown in [Figure 38 on page 163](#).

Figure 38: Export JMB to HTML Dialog Box



4. Click the **Original JMB** or **Filtered JMB** link to save the original or filtered JMB file as an HTML file.

To export an incident data as an Excel file:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select the incident whose details you want to export.
3. Select **Export Incident Summary to Excel** from the Actions menu or the shortcut menu.

The **Export Incident Summary to Excel** dialog box displays the Export the selected Incident to Excel link.

4. Click the **Export the selected Incident to Excel** link to save the incident data in Excel format.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Deleting an Incident

After reviewing the incident information, you can use the Incidents page to delete incidents from Service Now. This action deletes the incident both from the Service Now database and from the Incidents table.

To delete an incident:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents table appears.
2. Select the incident that you want to delete.
3. Click **Delete**.

The selected incidents are removed from the Incidents table and the Service Now database.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)

- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Submitting an Incident to Juniper Support Systems

After viewing an incident information, you can use the Incidents page to submit the incident to Juniper Support Systems (JSS) for creating a case. You can submit multiple incidents to JSS simultaneously. The status of a submitted incident appears in the Status column of the Incidents page. After you submit the incident, the status is Submitted. When a case is created by JSS, the status changes to Created and a case ID is generated for the incident.



NOTE: The Submitted status is displayed in red if an error or exception has occurred while submitting the incident to JSS. If you place the cursor on Submitted, a tool tip displays the error message.

An error or exception can occur while submitting an incident when there is an issue with Customer Relationship Manager (CRM) in JSS; for example, CRM is down for maintenance. The Submitted status is automatically displayed in black when the CRM becomes functional.

Before an incident is submitted from Service Now to JSS, the synopsis of the incident is tagged in the Service Now database to indicate whether it is an on-demand or a Return Materials Authorization (RMA) incident generated by AI-Scripts or Service Now. The synopsis of an incident generated by an event on a device is not tagged. An incident is submitted to JSS with one of the following tags:

- *AIS On Demand* for on-demand incidents generated by AI-Scripts
- *On Demand* for on-demand incidents generated by Service Now
- *Express RMA* for RMA incidents detected by AI-Scripts
- *On Demand RMA* for on-demand RMA incidents generated by Service Now

You can submit incidents to JSS as soon as a JMB is received from the device, without downloading attachments from the JMB. Then Service Now automatically uploads the JMB attachments to the related case.

To submit an incident to JSS:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. On the Incidents page, select the incident that you want to submit to JSS.
3. From the Actions menu, select **Submit Case**. Alternatively, right-click the incident and select **Submit Case**.

The Submit Case Options page appears as shown in [Figure 39 on page 166](#).



NOTE: The Submit Case action is disabled when you select an incident that is already submitted.

Figure 39: Submit Case Options Page

4. Click the **Enter Email Id** field to enter an e-mail ID in the user@example.com format.
5. (Optional) To add multiple e-mail IDs or delete them, use the **Add Email** and **Delete** buttons, respectively.
6. (Optional) Click **Modify** to modify the existing site ID or username.

The Make Selection to Change Site ID or User dialog box appears.

The site ID can be modified in two ways:

- For the same username:
 - a. Click **Default Org**.
 - b. Select a site ID from the Site ID list
- For a new user:

- a. In the **Username** field, enter the username to log in to an organization.

The username is provided by Juniper Networks or Juniper Networks Partner.

- b. In the **Password** field, enter the password to log in to an organization.

- c. Click the **Get Sites** link.

The Site ID list displays a list of site IDs.

- d. Select the required site ID.

7. (Optional) In the Make Selection to Change Site ID dialog box, select the **Save As Default User For Incident Submission** check box if you want the new site ID to be set as the default site ID. This new site ID and username are displayed by default when you log in next time to submit new incidents.

8. Click **OK** to save the changes and go back to the Submit Case Options page. Click **Cancel** if you do not want to implement the changes.

9. (RMA incident only) If you are submitting an RMA incident, on the Submit Case Options page, you must select an **Address Group**.

The **Ship-to Address** field is populated automatically based on the selected address group.

By default, in case of standard, partner proxy, or end customer modes, the Address Group field displays the address group values present in the system. The values displayed in the Address Group and Ship-to Address fields are determined by the following:

- In End Customer and Standard modes, the value displayed in the Address Group and Ship-to Address fields depend on the association between the device and address group. If a user has associated a device with an address group before the incident took place, then the value is preselected in the Address Group field. In case a user associates a device with an address group after the incident took place, then the Location and Ship-to Address fields display None. You can select any other address group present in the system to create a CRM case with JSS or a Juniper Networks Partner.
- In Partner Proxy mode, the Address Group and Ship-to Address fields are prepopulated with the address group sent by the customer and the address group present in the system for opening a case. A Juniper Networks partner has the option of changing this value by selecting an address group present in the partner system.
- If a Juniper Networks partner has associated an address with the End Customer device, then that address is displayed in the Address Group and Ship-to Address fields instead of the customer address.
- If no device is associated, the value displayed in the Address Group field is None.

The address group selected on the Submit Case page is submitted as the shipping address to a Juniper Networks partner or JSS.

10. Select the method for follow up on the case from the **Follow Up Method** list. The available options are Email Full Text Update, Email Secure Web Link, and Phone Call.

11. Enter a customer tracking number in the **Customer Tracking Number** field.

The customer tracking number can be any random number that you provide to track your case.



NOTE: Steps 4 through 11 are applicable only when you run Service Now in partner proxy or standard modes.

12. Select the priority of the case from the **Priority** list.

The available options are Critical, High, Medium, and Low. The default priority is Medium.

13. (Optional) Add your comments in the **Add Comments to Synopsis** field.

If you are submitting On-demand or Off-Box incidents to JSS, you can edit the default content in the Synopsis field.

14. (Optional) Add your comments in the **Add Comments to Description** field.

Ensure that your comments contain fewer than 1028 characters.

In Partner Proxy mode, a table listing core files for the incident is displayed below the Add Comments to Description field.

The columns in the table are described as follows:

- **Core Files**—Complete path to the core file, including the core filename
- **Core File Size(in bytes)**—Size of the core files, in bytes

15. Select one or more core files to upload. The core files are uploaded after the case is created for the incident.

16. (Optional) To delete core files from the router after uploading, select the **Delete Core Files from Router after Uploading** check box.

17. (Optional) To view the hardware components in the device, click the **Select Device Components** link next to the Synopsis field.

The Device Physical Inventory Components page appears.

18. Select the device components tofor requesting RMA incidents and click **Submit**.

19. In the **Problem Description** field, enter information about the device components (part number, version, part description, part serial number, and so on).

20. Click **Submit**.

A **Job Information** dialog box appears and displays the job ID.

Click the job ID to go to the **Job Management** page. You can monitor the status of the job from this page.

21. Navigate back to **Service Central > Incidents**.

The Incidents page appears.

22. On the Incidents page, click the RMA incident that you requested and select **Submit Case** from the Actions menu. Alternatively, right click the RMA incident and select **Submit Case**.

The Submit Case Options page appears.

23. Verify the information on the page and click **Save** to save your settings in the Service Now database and go back to the Incidents page.

24. Click **Submit** to submit the selected incident to JSS.

The Incidents page appears. The Incidents page displays the submission status in the Status column as Submitted.

When a case is created for the incident in JSS, the status of the incident changes to Created and a case ID is generated.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Viewing Incident Details on page 169](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Viewing Incident Details

When incidents are received, only selected information appears on the Incidents page. Using Service Now, you can view the entire content of the incident.

To view incident details:

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

The Incidents page appears.

2. Double click on an incident to view its details. The **Incident Detail** page appears.



NOTE: If the selected incident type is Event (low end), the Problem Description field in the Incidents Detail page highlights the low end JMB with the note section that contains the following information: *This incident is based on a "low impact" JMB. A low impact JMB was generated to preserve system resources on the network node. Low impact JMBs do not include all the troubleshooting information found in a traditional JMB. A list of command output recommended for this event, but not contained in the low impact JMB, is listed below. If you open a case with this incident you can attach the recommended command output to the case by clicking the Incident and then the "view in case manager" action in Service Now.*

AI-Scripts adds this content when generating event based JMBs or eJMBs.

The **Incident Detail** page displays the following tabs: Incident Details, Case Details, Core File Details, Attachment Details, and Log File Details as shown in [Figure 40 on page 170](#). The **End-Customer Case Details** tab appears in the partner proxy mode for end customer incidents.

Figure 40: Incident Detail Page

The screenshot shows the 'Incident Detail' page with the following tabs: Incident Details (selected), Case Details, Core File Details, Attachment Details, and Log File Details. The main content area displays the following information:

- Device: device1
- IP Address: 192.0.100.0
- Device Serial Number:
- Product: EX-XRE
- Platform: junos-ex
- Release: 12.3R6
- Version: R6
- Organization: Test-Organization
- Device Group: Device Group for Test-Organization
- Occurred: Feb 11, 2014 2:15:51 PM IST
- Status: Submitted
- Incident ID: device1-999-2014011-004549-999
- Event Type: -
- Defect Type: -

At the bottom, there is a section for 'KB Article: None'.

You can retrieve required information from the tabs.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)

- [Viewing Knowledge Base Articles Associated with an Incident on page 171](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Viewing Knowledge Base Articles Associated with an Incident

Knowledge Base provides information about the causes and solutions for a problem. Using Service Now you can view Knowledge Base (KB) articles associated with an incident.

To view the KB article associated with an incident:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents table appears.
2. Select an incident to view the KB article associated with it, and select **View KB Article** from either the **Actions** list or the right-click menu.

A new window takes you to the Juniper Networks Knowledge Base article page where you can log in and view the KB article.



NOTE: This action is disabled for incidents that do not have any associated Knowledge Base (KB) articles.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing a Case in the Case Manager on page 171](#)
- [Updating an End-Customer Case on page 172](#)

Viewing a Case in the Case Manager

You can view the details of a submitted case in the Juniper Networks Case Manager. To view case details in the Case Manager, you must first have a user ID and password for the Juniper Networks Customer Support Center (CSC). You can request the user ID and password at <http://www.juniper.net/customers/support/> or by contacting Juniper Networks Customer Care.



NOTE: This feature is not available if Service Now is in offline mode.

To view a case in the Case Manager:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select the incident whose details you want to view in the Case Manager, and select **View Case in Case Manager** from either the **Actions** list or the right-click menu.

The Juniper Networks Login page appears.



NOTE: If the **View Case in Case Manager** link is not enabled, verify if the case is created.

3. Enter your username and password and click **Login**.

The JSS Case Manager displays the case details.



NOTE: You can also view the details of the submitted cases in the Case Manager from the View Tech Support Cases page. To view case details, go to **Service Central > Incidents > View Tech Support Cases**.

Related Documentation

- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Updating an End-Customer Case on page 172](#)

Updating an End-Customer Case

In Partner Proxy mode, you can create a case for the incident you receive from an end-customer's device and also update the case.



NOTE: This action is enabled only when Service Now operates in partner-proxy mode and when the state of the selected case is open.

To update an end-customer case:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page displays the list of incidents.
2. Select the end-customer incident for which you want to create a case, and select **End-Customer Case** from either the **Actions** list or the right-click menu.
The **End-Customer Case** dialog box appears as shown in [Figure 41 on page 173](#).

Figure 41: End-Customer Cases Dialog Box

The screenshot shows a dialog box titled "End Customer Cases". It contains the following fields and controls:

- Case ID:** ECC1
- Case Link:** An empty text input field.
- Case Status:** A dropdown menu currently showing "Updated".
- Synopsis:** CHASSISD_FRU_OFFLINE_NOTICE
- Problem Description:** A section with two parts:
 - Event message:** CHASSISD_FRU_OFFLINE_NOTICE
 - Event description:** The chassis process (chassisd) took the indicated component (FPC3) offline for the
- Email List:** user@example.com
- Buttons:** Submit and Cancel at the bottom right.

This **End-Customer Case** action is enabled only if you select an end-customer incident.

3. Modify the case details as necessary.
4. Click **Submit**.

The case is updated and sent to the Service Now end-customer.

Related Documentation

- [Service Now Overview on page 34](#)
- [Adding a Connected Member on page 77](#)
- [Incidents Overview on page 158](#)
- [Assigning an Incident Owner on page 160](#)
- [Flagging an Incident to a User on page 161](#)
- [Deleting an Incident on page 164](#)
- [Checking Incident Status Updates on page 162](#)
- [Exporting Incident Data on page 163](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Viewing Incident Details on page 169](#)
- [Viewing a Case in the Case Manager on page 171](#)

Uploading Core Files for Incidents

Using Service Now, you can upload core files generated for an event to JSS. This function is supported under the following conditions:

- Case should be created for the incident
- At least one core file should be available for upload

If there are no core files available for the incident or if all the core files are uploaded, then this action is disabled in **Incidents**.

To upload core files:

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

The **Incidents** page appears.

2. Select the incident whose core files you need to upload, and select **Upload Core Files** from either the **Actions** list or the right-click menu.



NOTE: This action is available only if the incident has any core file to be uploaded. In addition, this action is disabled in the offline and the demo modes.

The **Core File Uploader** dialog box appears with a list of core files.

3. Select the core files that you want to upload, and click **Submit**.
4. If you need to delete the core files from router after uploading, select the **Delete Core Files from Router after Uploading** check box.

Related Documentation

- [Incidents Overview on page 158](#)
- [Submitting an Incident to Juniper Support Systems on page 165](#)
- [Uploading Core Files Generated for Events on page 133](#)
- [Updating Core File Upload Configuration on page 82](#)

Information

- [Messages Overview on page 175](#)
- [Assigning Ownership on page 175](#)
- [Flagging a Message to Users on page 176](#)
- [Deleting a Message on page 177](#)
- [Scanning a Message for Impact on page 177](#)
- [Assigning a Message to a Connected Member on page 178](#)
- [Device Snapshots Overview on page 180](#)

- [Exporting Device Data to HTML on page 181](#)
- [Deleting Device Snapshots on page 182](#)
- [Viewing Device Snapshot Details on page 182](#)

Messages Overview

Service Now polls JSS regularly for information messages for every configured organization. These information messages are displayed on the Service Now Messages page. Using Service Now, you can assign an owner to an information message and flag it to users. This ensures that users are kept informed of changes made to information messages.

You can perform the following tasks in the Information Messages tab:

- Assign an owner to an information message
- Assign messages to connected members
- Flag an information message to users
- Delete information messages
- Scan for affected devices

Related Documentation

- [Device Snapshots Overview on page 180](#)
- [Assigning Ownership on page 175](#)
- [Flagging a Message to Users on page 176](#)
- [Scanning a Message for Impact on page 177](#)
- [Deleting a Message on page 177](#)

Assigning Ownership

You can assign an owner to every information message for managing any follow up task pertaining to the message.

To assign an owner to an information message:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.
The Messages page appears.
2. Select the information message to which you want to assign an owner, and select **Assign Ownership** from either the **Actions** list or the right-click menu.
The **Assign Ownership** dialog box appears.
3. Enter the login ID of the new owner in the **Enter the Login ID of User** field.
4. Select the **Email Message to Assigned Owner** check box to send an e-mail notification to the assigned owners of the message. This option is selected by default.
5. Click **Submit**.

The specified user is assigned ownership of the selected information message.

- Related Documentation**
- [Flagging a Message to Users on page 176](#)
 - [Scanning a Message for Impact on page 177](#)
 - [Deleting a Message on page 177](#)
 - [Assigning a Message to a Connected Member on page 178](#)
 - [Viewing Messages Assigned to a Connected Member on page 81](#)
 - [Messages Overview on page 175](#)
 - [Device Snapshots Overview on page 180](#)

Flagging a Message to Users

You can flag an information message to a Junos Space user who you think needs to keep track of the information message or who needs to be notified when it is changed.

To flag an information message to a user:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.

The Messages page appears.

2. Select the information message that you want to flag to a user, and select **Flag to Users** from either the **Actions** list or the right-click menu.

The **Flag to Users** dialog box lists the available users.

3. Select one or more users who must be notified of the selected information message.
4. Select the **Email Message to Flagged Users** check box to send an e-mail notification to all the flagged users of the message. This option is selected by default.
5. Click **Submit**.

The specified users are notified of the selected information message and the **Flag** column of that information message displays **Yes**.

- Related Documentation**
- [Device Snapshots Overview on page 180](#)
 - [Assigning Ownership on page 175](#)
 - [Scanning a Message for Impact on page 177](#)
 - [Deleting a Message on page 177](#)
 - [Assigning a Message to a Connected Member on page 178](#)
 - [Viewing Messages Assigned to a Connected Member on page 81](#)
 - [Messages Overview on page 175](#)

Deleting a Message

You can delete information messages from the Service Now database that Service Now collects and that are displayed on the Messages page.

To delete an information message:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.
The Messages page appears.
2. Select the information message that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.
3. Click **Delete** again to confirm the deletion.

The selected information messages are deleted from the Service Now database and they no longer appear on the Messages page.

Related Documentation

- [Device Snapshots Overview on page 180](#)
- [Assigning Ownership on page 175](#)
- [Flagging a Message to Users on page 176](#)
- [Scanning a Message for Impact on page 177](#)
- [Assigning a Message to a Connected Member on page 178](#)
- [Viewing Messages Assigned to a Connected Member on page 81](#)
- [Messages Overview on page 175](#)

Scanning a Message for Impact

You can use Service Now to view the devices impacted by the vulnerabilities described in the information message.

To scan iJMBs and view the impacted devices:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.
The Messages page appears.
2. Select the message that you want to scan for impact, and select **Scan for Impact** from either the **Actions** list or the right-click menu.

The Scan for Impact Results page displays the list of devices that are impacted by the selected message. If no devices are impacted by the selected message, the following message appears:

No impacted devices found.

Related Documentation

- [Device Snapshots Overview on page 180](#)
- [Assigning Ownership on page 175](#)
- [Flagging a Message to Users on page 176](#)

- [Deleting a Message on page 177](#)
- [Assigning a Message to a Connected Member on page 178](#)
- [Viewing Messages Assigned to a Connected Member on page 81](#)
- [Messages Overview on page 175](#)

Assigning a Message to a Connected Member

Service Now polls JSS regularly to receive messages for every configured organization. As a Service Now partner, you can assign multiple messages to a connected member.



NOTE: This action is available only when Service Now operates in partner-proxy mode. For more information about standard, partner-proxy, and end-customer modes, see [“Service Now Modes” on page 42](#).

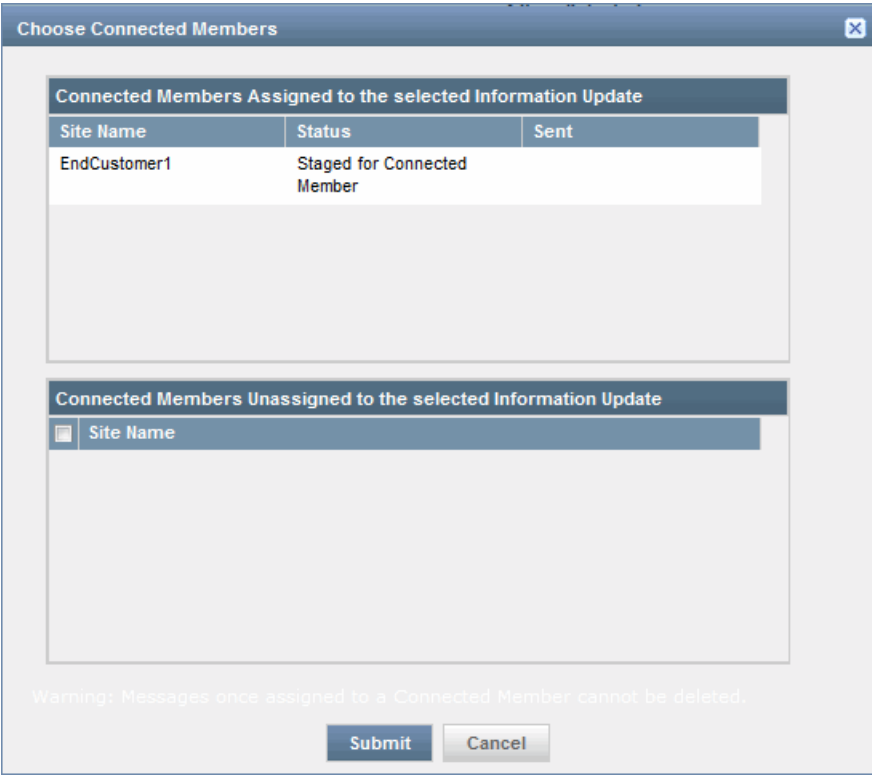
After a message is assigned to a connected member, it cannot be deleted.

To assign a message to a connected member:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.
The Messages page displays the list of information messages received.
2. Select the message that you want to assign to a connected member, and select **Assign Message to End-Customer** from either the **Actions** list or the right-click menu.

As shown in [Figure 42 on page 179](#), the **Choose Connected Members** dialog box displays the list of connected members. It also displays the connected members to whom the message is already assigned along with the status (if any).

Figure 42: Choose Connected Members Dialog Box



The dialog box is titled "Choose Connected Members" and contains two main sections. The first section, "Connected Members Assigned to the selected Information Update", displays a table with the following data:

Site Name	Status	Sent
EndCustomer1	Staged for Connected Member	

The second section, "Connected Members Unassigned to the selected Information Update", contains a search bar with the label "Site Name". At the bottom of the dialog, there is a warning message: "Warning: Messages once assigned to a Connected Member cannot be deleted." and two buttons: "Submit" and "Cancel".

3. Select the connected member to whom this message must be assigned.
4. Click **Submit**.

The selected message is assigned to the connected member. To verify this action, select **Administration > Organization** to navigate to the Organizations page, and list the messages assigned to any connected member. See [“Viewing Messages Assigned to a Connected Member”](#) on page 81.

Related Documentation

- [Adding a Connected Member on page 77](#)
- [Device Snapshots Overview on page 180](#)
- [Assigning Ownership on page 175](#)
- [Flagging a Message to Users on page 176](#)
- [Scanning a Message for Impact on page 177](#)
- [Deleting a Message on page 177](#)
- [Viewing Messages Assigned to a Connected Member on page 81](#)
- [Messages Overview on page 175](#)

Device Snapshots Overview

Service Now periodically collects and displays Information Juniper Message Bundles (iJMBs) that contain information about devices. iJMBs are also called device snapshots. They are processed and displayed on the Device Snapshot page in the Service Now application. You can upload these device snapshots to JSS where they are added to the Customer Intelligence Database (CIDB) and then processed and analyzed to provide preventive measures.

You can filter the configuration content from device snapshots that are sent to JSS by setting the JMB Filter Level while creating the organization (See [“Adding an Organization” on page 75](#)) and then track the status of the device snapshot submission to JSS. You can also stop device snapshots from being sent to JSS.

After you install AI-Scripts on a device, device snapshots are sent from each device to Service Now and from Service Now to JSS every 7 days. The configuration information in a device snapshot that is shared with JSS depends on the **JMB Filter Level** settings made while creating the organization to which the devices belongs.

The device snapshots that are received by Service Now and yet to be submitted to JSS are stored with the status **Initial**. After the 7 days elapse, the latest device snapshot sent from the device is submitted to JSS. This means that when a device sends multiple device snapshots to Service Now, only the most recent device snapshot is submitted to JSS and the remaining device snapshots are denoted with the status **Skipped**. Device snapshots are denoted with the Initial status for several reasons. To know why a device snapshot is not submitted to JSS, you can hover over its **Status** in the tabular view of the Device Snapshot page. The **Status** field also displays additional information such as the reasons for not loading information JMBs and messages for errors that might have occurred while loading the JMB.

Devices that have stopped sending iJMBs (device snapshots) to Service Now for more than two weeks are also detected and graphically displayed on the Administration page. To list these devices, you can click the Devices Not Sending Snapshots bar of the Devices Not Sending Device Snapshots graph. These devices are displayed on the Service Now Devices page where you can view their details and export them to HTML format. The Quick View of the Device Snapshots page uses different icons to help you identify snapshots that are successfully uploaded to JSS and the device snapshots that could not be uploaded to JSS. For a description of these icons, see *Service Now Icons and Inventory Pages* .

Service Now generates iJMBs automatically for all devices associated to a device group when the devices stop sending iJMBs. The iJMBs are generated based on the commands available in a directive file pre-loaded in Service Now. The behavior of these iJMBs is the same as the iJMBs generated by event scripts. The Service Now administrator receives a message when Service Now generates iJMBs automatically for one or more devices.

Service Now generates iJMBs automatically if:

- Service Now detects that a Junos upgrade has occurred but an event profile is reinstalled, or if Service Now detects that the device has not sent an iJMB for some time
- an event profile was never installed on a device, but the device is associated to a device group in Service Now

If an event profile is installed on the device and an iJMB is received from the device, then Service Now stops creating iJMBs for the device. If the notification policy **Switch over enabled for iJMB** is enabled, the administrator is notified by an e-mail or an SNMP Trap when Service Now generates iJMBs for one or more devices. If the notification policy **Switch over enabled for iJMB** is not enabled, only e-mails are sent to the administrator when Service Now generates iJMBs. No SNMP traps are sent.

You can perform the following tasks using the Information Device Snapshots tab:

- Export device data in HTML format
- Delete a device snapshot
- View device snapshot details

Related Documentation

- [Exporting Device Data to HTML on page 181](#)
- [Deleting Device Snapshots on page 182](#)
- [Viewing Device Snapshot Details on page 182](#)
- [Messages Overview on page 175](#)

Exporting Device Data to HTML

You can store the device data that Service Now collects and displays on the Device Snapshots page and export it to HTML format.

To export device data to HTML format:

1. From the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.

The Device Snapshots page displays the device snapshots received.

2. Select the organization whose data you want to export, and select **Export to HTML** from either the **Actions** list or the right-click menu.

The **Export JMB to HTML** dialog box displays links to the original and filtered versions of the JMB.

3. Click the displayed link to save the iJMB as an HTML file.

Related Documentation

- [Device Snapshots Overview on page 180](#)
- [Deleting Device Snapshots on page 182](#)

- [Viewing Device Snapshot Details on page 182](#)
- [Messages Overview on page 175](#)

Deleting Device Snapshots

You can take device data that Service Now collects and displays on the Device Snapshots page and delete it from the Service Now database.

To delete an iJMB:

1. From the Service Now navigation tree, select **Service Central** > **Information** > **Device Snapshots**.

The Device Snapshots page appears.

2. Select the organization whose device information you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.
3. Click **Delete** again to confirm the deletion.

The iJMBs from the selected organizations are deleted from the Service Now database and they no longer appear on the Device Snapshots page.

Related Documentation

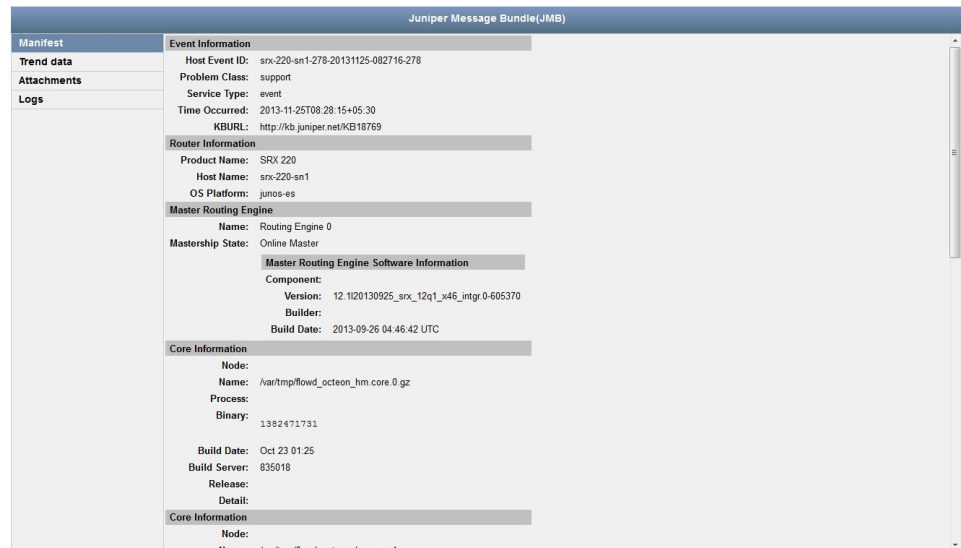
- [Device Snapshots Overview on page 180](#)
- [Exporting Device Data to HTML on page 181](#)
- [Viewing Device Snapshot Details on page 182](#)
- [Messages Overview on page 175](#)

Viewing Device Snapshot Details

When Service Now receives JMBs, only selected information from the JMBs appears on the Device Snapshots page. However, you can view the entire contents of the JMB on the View JMB page.

Service Now displays the JMBs generated by AI-Scripts Release 3.7 and earlier on a single page. For JMBs generated by AI-Scripts Release 4.0 and later, the View JMB page has a right and a left pane. The left pane lists the sections of a JMB. Clicking a section displays the contents of the section in the right pane. When the View JMB page opens, by default, the Manifest section opens as shown in [Figure 43 on page 183](#). You can click the links in the Attachments and Logs sections to view or download the attachment and log files.

Figure 43: Juniper Message Bundle



To view details of a JMB:

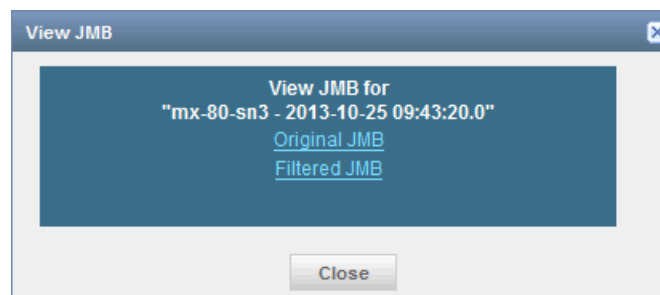
1. From the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.

The Device Snapshots page appears.

2. On the Device Snapshots page, select the device for which you want to view JMB.
3. From the Actions menu, select **View JMB**. Alternatively, right-click the device and select **View JMB**.

The **View JMB** dialog box displays links to the original and the filtered JMBs as shown in Figure 44 on page 183. The information in the filtered JMB is classified by the settings on your Global Settings page.

Figure 44: View JMB Dialog Box



4. Click a link to view the JMB details.

Related Documentation

- [Device Snapshots Overview on page 180](#)
- [Exporting Device Data to HTML on page 181](#)
- [Deleting Device Snapshots on page 182](#)

- [Messages Overview on page 175](#)

JMB Errors

- [JMBs with Errors on page 184](#)

JMBs with Errors

Service Now considers a Juniper Message Bundle (JMB) as erroneous if it does not comply with the standard data structure that Service Now accepts or if the Manifest section of the JMB is incorrect. From AI-Scripts Release 4.0, an incomplete Trend section or attachment in the JMB is ignored.

Service Now identifies the JMBs with errors and displays them on the JMB Errors page. You can download up to five JMB files at a time and also delete them from the Service Now database. We recommend that you open a case with JSS for JMBs with errors.

Refer to the following topics to download or delete JMBs with errors:

- [Downloading JMBs with Errors on page 184](#)
- [Deleting JMBs with Errors on page 185](#)

Downloading JMBs with Errors

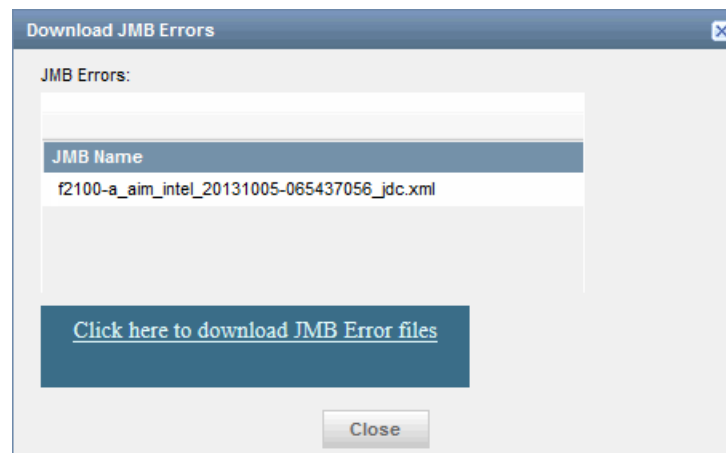
When you download a JMB, it is saved as a zip file. You can download up to five JMBs with errors at a time.

To download JMBs with errors:

1. From the Service Now navigation tree, select **Service Central > JMB Errors**.
The JMB Errors page appears.
2. On the JMB Errors page, select the JMBs that you want to download.
3. From the Actions menu, select **Download JMB Errors**. Alternatively, right-click the selected JMBs and select **Download JMB Errors**.

The **Download JMB Errors** dialog box appears as shown in [Figure 45 on page 185](#)

Figure 45: Download JMB Errors Dialog Box



4. Click the **Click here to download JMB Error files** link to save the selected JMBs with errors.

Your browser opens a dialog box prompting you to open or save the zip file.

5. Select **Save** to save the file on your local system.
6. Click **OK**.

A dialog box appears to allow you to browse the location where you want to save the file.

7. Click **Save**.

The file is saved on your local system.

Deleting JMBs with Errors

You can delete multiple JMBs with errors at the same time.

To delete JMBs with errors:

1. From the Service Now navigation tree, select **Service Central > Incidents > JMB Errors**.
The JMB Errors page appears.
2. On the JMB Errors page, select one or more JMBs that you want to delete.
3. From the Actions menu select **Delete**. Alternatively, right-click and select **Delete**.
The Delete Error JMB dialog box prompts you to confirm the deletion.
4. Click **Delete**.

The selected error JMBs are deleted from the Service Now database and they no longer appear on the JMB Errors page.

- Related Documentation**
- [Service Central Overview on page 155](#)
 - [Messages Overview on page 175](#)

Notifications

- [Notification Policies Overview on page 186](#)
- [Creating and Editing a Notification Policy on page 187](#)
- [Enabling or Disabling a Notification Policy on page 194](#)
- [Deleting a Notification Policy on page 194](#)

Notification Policies Overview

Service Now sends a notification to users when a specific event occurs. Notification policies define the parameters for these notifications. A notification policy specifies the events for which you want Service Now to send a notification. It also specifies the actions a user must take for that event.

You must specify the following parameters when you create a notification policy:

- **Trigger**—the event that causes Service Now to send notification.
- **Filters**—Specify filters for the events that cause Service Now to send a notification.
- **Actions**—Specify the action (or actions) that must be taken after the specified event occurs. These events can be filtered by priority, device name, serial number, and so on. Different filters are supported for incident and information trigger types.

The Notifications page displays the notification policies chronologically by name, owner, status, and trigger. For more information about the Notifications table columns, see [Table 19 on page 186](#).

Table 19: Notification Policies Table Column Descriptions

Element Name	Description	Privilege Required to Modify	Range/Length
Name	Name of the policy.	Hyperlink requires Notification Policy privilege	64 characters
Owner	Name of the user who owns the notification policy.	—	—
Status	Whether the notification policy is running.	—	Enabled or Disabled

Table 19: Notification Policies Table Column Descriptions (*continued*)

Element Name	Description	Privilege Required to Modify	Range/Length
Trigger Type	<p>Type of the trigger for which the notification policy is applied.</p> <ul style="list-style-type: none"> • New Incident Detected • Incident Submitted • Case ID Assigned • New Exposure • Service Contract Expiring • Case Status Updated • New Intelligence Update • Ship-to Address Missing For Device • Switch over enabled for IJMB • Connected Member Device Added/Removed 	–	

**NOTE:**

- If **Ship-to Address Missing For Device** is configured, Service Now sends notification when RMA cases are submitted without any address getting associated to it.
- **New Incident Detected** is the only option available when Service Now is in offline mode.
- If **Switch over enabled for IJMB** is configured, Service Now automatically generates IJMBs for the device (associated to a device group) that do not send IJMBs.
- **Connected Member Device Added/Removed** is a notification trigger added if Service Now operates in the partner proxy mode Service Now to notify when devices are added or removed by a connected member.

Related Documentation

- [Creating and Editing a Notification Policy on page 187](#)
- [Enabling or Disabling a Notification Policy on page 194](#)
- [Deleting a Notification Policy on page 194](#)

Creating and Editing a Notification Policy

Notification policies specify when you want Service Now to send notifications about an event and the recipients of the notifications. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

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 46 on page 188](#),

Figure 46: Create Notifications Page

2. Enter a notification policy name, and select a trigger.

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

3. Expand the Apply Filters section, if not already expanded, and enter the filter parameters.

Different filters are supported for incident and information trigger types.

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

For more information about the fields in the **Create Notifications** dialog box, see [Table 20 on page 189](#).

5. Specify the destinations where SNMP traps can be sent when an event occurs in the **Send SNMP Traps to** section.

For more information about the fields in the **Create Notifications** dialog box, see [Table 20 on page 189](#).

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

7. Click **Add**.

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

You can also copy an existing notification policy and modify its attributes to create another notification policy.



NOTE: While copying a notification policy, you cannot edit the **Trigger** field.

To copy a notification policy:

1. From the Service Now navigation tree, select **Service Central > Notifications**.
The Notifications page appears.
2. Select the notification policy that you want to copy, and select **Copy** from either the **Actions** list or the right-click menu.
The Copy Notifications page appears.
3. Make your modifications.
4. Click **Make a Copy**.

A notification policy is created with the settings that you specified and listed in the Notifications page.

To modify a notification policy:

1. From the Service Now navigation tree, select **Service Central > Notifications**.
The Notifications page appears.
2. Select the notification policy that you want to edit, and select **Edit filters and Actions** from either the **Actions** list or the right-click menu.
The Edit Notifications page appears.
3. Edit the desired fields. For more information, see [Table 20 on page 189](#).

Table 20: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Remark
Name	Enter a unique name for the policy.	64 characters	—

Table 20: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
Trigger Type	Enter the type of trigger required to activate this policy. The fields in the filter table dynamically change according to the selected trigger type.	New Incident Detected	This is the only option available when Service Now is in offline mode.
		Incident Submitted	
		Case ID Assigned	
		Case Status Updated	
		New Intelligence Update	
		Service Contract Expiring	
		New Exposure	
		Ship-to Address Missing For Device	If this notification is enabled, Service Now will send notification when RMA cases get submitted without the address getting associated to it.
		Switch over enabled for IJMB	If this notification is enabled, the switch over e-mail/SNMPtraps will be sent as per the policy configured. If this policy is not configured, only e-mail will be sent to the Service Now admins configured in space.
		Connected Member Device Added/Removed	

Table 20: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
			Notification added in Partner Proxy Service Now for devices added or removed by a connected member.
Apply Filters:			
NOTE: You can select either Organization or Device Group when creating or modifying a notification.			
Filter Parameters for New Incident Detected, Incident Submitted, Case ID Assigned, Case Status Updated and Ship-to Address Missing Triggers:			
Priority	Select a value in the Priority field. Service Now sends a notification if the priority of the incident matches the entered value.	255 characters	Blank
Organization	Select a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.	255 characters	Blank
Device Group	Select a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.	255 characters	Blank
Device Name	Enter a value in the Device Name field. Service Now sends a notification if the name of the device the incident occurred on matches the entered value.	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value.	255 characters	Blank
Has the words	Enter a value in the Has the words field. Service Now sends a notification if the specified words match any of the fields in the incident or the information message.	255 characters	Blank
Does not have	Enter a value in the Doesn't have field. Service Now sends a notification if the specified words do not match any of the fields in the incident or the information message.	255 characters	Blank
Filter Parameters for New Intelligence Update Triggers:			

Table 20: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
Intelligence Update Type	Enter a value in the Intelligence Update Type field. Service Now sends a notification if the type of information message update matches the entered value.	255 characters	Blank
Products Affected	Enter a value in the Products Affected field. Service Now sends a notification if the Products Affected field value in alert information messages matches the entered value.	255 characters	Blank
Platform Type	Enter a value in the Platform Type field. Service Now sends a notification if the Platforms Affected field in alert information messages or the platform type field in information messages match the entered value.	255 characters	Blank
Keywords	Enter a value in the Keywords field. Service Now sends a notification if the Keyword in information messages matches the entered value.	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value.	255 characters	Blank
Software Version	Enter a value in the Software Version field. Service Now sends a notification if the software version in the information messages matches the entered value.	255 characters	Blank
Organization	Enter a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.		
Device Group	Enter a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.		
Devices Impacted	Enter a value in the Devices Impacted field. Service Now sends a notification if the devices impacted in the information messages matches the entered value.	255 characters	Blank
Has the words	Enter a value in the Has the words field. Service Now sends a notification if the specified words match any of the fields in the incident or the information message.	255 characters	Blank
Does not have	Enter a value in the Doesn't have field. Service Now sends a notification if the specified words do not match any of the fields in the incident or the information message.	255 characters	Blank
Filter Parameters for Service Contract Expiring Triggers:			
Organization	Enter a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.		

Table 20: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
Device Group	Enter a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.		
Device Name	Enter a value in the Device Name field. Service Now sends a notification if the name of the device the incident occurred on matches the entered value.	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value.	255 characters	Blank
Filter Parameters for New Exposure Triggers:			
Organization	Enter a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.		
Device Group	Enter a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.		
Devices	Enter a value in the Devices field. Service Now sends a notification if the name of the device the incident occurred on matches the entered value.	255 characters	Blank
Actions:			
Send Email to	Specify the e-mail addresses of users who must receive an alert if the policy is triggered and matches the specified filter. To add a new e-mail address to the list, click Add Email . Click the Enter Email Id field to enter the e-mail address. The e-mail address should be in the format user@example.com. To delete an e-mail address from the list, select the e-mail address and click Delete .	65535 characters	Blank
Send Traps to	Specify the destinations where SNMP traps can be sent when an event occurs and matches the specified filter. See "Adding an SNMP Server" on page 129 .	–	–

- Related Documentation**
- [Notification Policies Overview on page 186](#)
 - [Enabling or Disabling a Notification Policy on page 194](#)
 - [Deleting a Notification Policy on page 194](#)

Enabling or Disabling a Notification Policy

Notification policies specify the events for which Service Now sends notifications, as well as the actions that Service Now takes in response to these events. They define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

To enable a notification policy:

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

The Notifications page appears.

2. Select the notification policies that you want to enable or disable, and select **Enable/Disable** from either the **Actions** list or the right-click menu.

The **Change Reaction Policies Status** dialog box appears and displays the name and status of the selected incident.

3. Click **Change Status** to confirm your action.

The status of the notification policy is changed.

Related Documentation

- [Notification Policies Overview on page 186](#)
- [Creating and Editing a Notification Policy on page 187](#)
- [Deleting a Notification Policy on page 194](#)

Deleting a Notification Policy

A notification policy specifies the events for which Service Now sends notifications, and the actions that Service Now takes in response to these events. It defines the events that trigger the notification, the filters that further specified the trigger events, and the actions that you want Service Now to take after the event is triggered.

To delete a notification policy:

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

The Notifications page appears.

2. Select the notification policy that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.

The **Confirm Deletion of Notification Policies** dialog box displays the name of the notification policy and its owner.

3. Click **Delete**.

This action deletes the selected notification policies from the Service Now database and from the Notifications page.

Related Documentation

- [Notification Policies Overview on page 186](#)

- [Creating and Editing a Notification Policy on page 187](#)
- [Enabling or Disabling a Notification Policy on page 194](#)

PART 3

Junos Space Service Insight

- [Introduction to Service Insight on page 199](#)
- [Insight Central on page 207](#)

CHAPTER 8

Introduction to Service Insight

- [Service Insight Overview on page 199](#)

Service Insight Overview

- [Service Insight Overview on page 200](#)
- [Service Insight Domain Overview on page 205](#)

Service Insight Overview

Service Insight is an application that helps in accelerating operational analysis and managing the exposure to known issues. Using Service Insight, you can identify devices that are nearing their End Of Life (EOL) and also discover and prevent issues that could occur in your network. The functionality of Service Insight is dependent on the information sent from Service Now. To enable Service Insight, you must add a valid organization in the Service Now application. See the [“Adding an Organization” on page 75](#) section in the *Junos® Space Service Now User Guide*.

Service Insight identifies the devices available for EOL reports and enables you to generate EOL reports that provide detailed device EOL information about EOL devices, such as the number of devices with EOL parts, EOL announce date, number of EOL announce parts, End Of Engineering SW date, number of End Of Engineering SW parts, End Of Engineering HW date, number of End Of Engineering HW parts, End Of Support date, number of End Of Support parts, top-level assembly parts, circuit assembly parts, PSN numbers, and replacement numbers. See [“Exposure Analyzer Overview” on page 208](#).

Service Insight provides Proactive Bug Notifications (PBNs) as a proactive measure to alert you about known issues that can impact the devices in your network. It is an effective means of communicating the information collected while helping one customer fix issues to another customer who could face similar issues in future. Using this information, which was collected when issues were reported to Juniper Networks, Service Insight identifies devices on your network with similar conditions. PBNs associated with devices on your network are matched and displayed on the **Manage PBNs** page. These PBNs keep you aware of the possible impacts and also of ways to fix the issue. PBNs also consist of workarounds that suggest temporary fixes and instructions that you can follow to protect your network. See [“Targeted PBNs Overview” on page 220](#).

Juniper Care Plus customers are entitled to receive PBNs that are managed by the Advanced Services (AS) team. Juniper Care customers are entitled to receive only auto PBNs. Auto PBNs are PBNs that are generated automatically by the system. They are not managed by the AS team. Customers who do not have JCare Plus license are considered as JCare customers.

Service Insight receives updates about EOL and PBN information. It also enables you to send notifications about these updates to multiple users and manage these notifications. You can define the events that trigger a notification, the filters that further specify the trigger events, and also the actions that you want Service Insight to take after the notification is triggered. See [“Notifications Overview” on page 224](#).

Service Insight uses two timers, one that runs every midnight, and another that runs every hour. The hourly timer initiates the processing of pending EOL requests. This timer schedules when JSS must send these requests to the corresponding devices. When large number of devices is added to Service Insight, JSS sends these requests in batches. The timer that runs every midnight updates the EOL and PBN data by sending requests to JSS and processing the responses that are received from JSS. This timer also initiates the synchronization process between Service Now and Service Insight which enables Service Insight to display the changes that were made to devices in Service Now. When you execute device related actions in Service Now while either one of these timers is running, Service Insight takes an hour to display the changes corresponding to these actions.

- [Service Insight Dashboard Overview on page 202](#)
- [Dashboard Gadgets on page 202](#)

Service Insight Dashboard Overview

The Service Insight dashboard displays notifications and graphically illustrates the number of devices per device group and the number of devices not sending device snapshots. You can access the Service Insight dashboard by selecting **Service Insight** from the **Application Switcher**.

The Service Insight dashboard includes:

- [Service Insight Workspaces on page 202](#)

Service Insight Workspaces

Apart from the Insight Central and Administration workspaces, Service Insight also provides shortcuts to the Devices and Jobs workspaces by including them in the Service Insight navigation tree. [Table 21 on page 202](#) lists the tasks that can be performed using the Service Insight workspaces.

Table 21: Service Insight Workspaces

Workspace Name	Tasks Included
Insight Central	<p>Using the Insight Central workspace, you can perform the following tasks:</p> <ul style="list-style-type: none"> • View devices for which EOL reports and associated PBNs are available.. • Generate EOL reports. • Identify PBNs that can affect specific devices. • View list of PBNs associated with devices added in the Service Now application. • Flag PBNs to users. • Assign ownership of PBNs. • E-mail PBN details to users. • Delete PBNs.
Administration (Service Now workspace)	<p>Using the Administration workspace you can perform the following tasks:</p> <ul style="list-style-type: none"> • Add and manage devices. Adding devices enables you to receive EOL and PBN data for those devices. • Manage script bundles and install and uninstall AI-Scripts on devices. • Add and manage device groups. • Add and manage Service Now organizations. • Configure Service Now global settings.

Dashboard Gadgets

The dashboard displays gadgets with information that is updated automatically and instantaneously. You can move gadgets on the dashboard and change their sizes. These

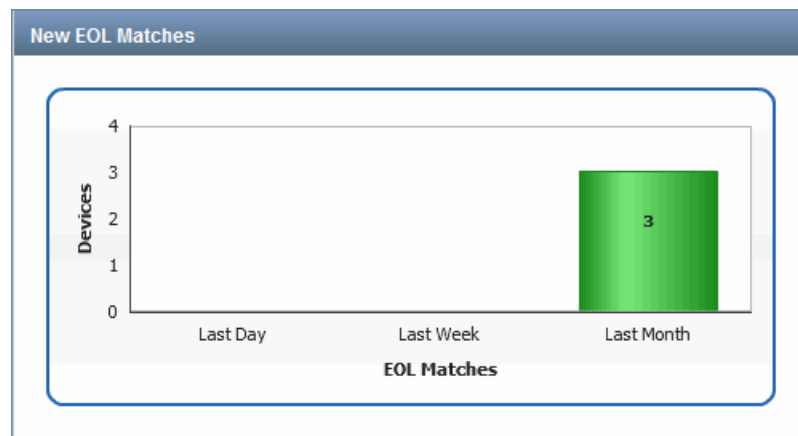
changes persist even after you log back in to the system. The gadgets displayed on the Service Insight dashboard are:

- [New EOL Matches on page 203](#)
- [Recent PBNs on page 203](#)
- [PBN Severity on page 204](#)
- [Service Insight Notices on page 204](#)

New EOL Matches

The **New EOL Matches** gadget graphically displays the EOL matches found for the devices on the previous day, the previous week, and the past month. Clicking a bar within the graph takes you to the **Exposure Analyzer** page which displays the devices for which the EOL matches are found.

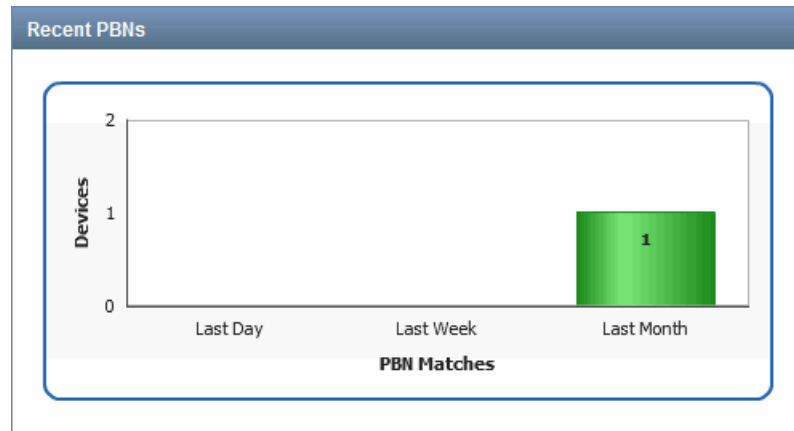
For example, when you click the green bar of the **New EOL Matches** gadget (as shown in the following figure), the **Exposure Analyzer** page displays only the two devices for which EOL notifications were received last month.



Recent PBNs

The **Recent PBNs** gadget graphically displays the devices for which PBNs were received the previous day, the previous week, and the past month. Clicking the bars within the graph takes you to the **Manage PBNs** page which lists the devices for which the PBNs are found.

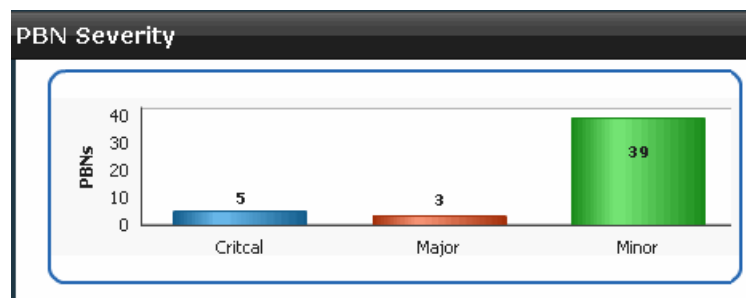
For example, when you click the green bar of the **Recent PBNs** gadget (as shown in the following figure), the **Manage PBNs** page lists only those three devices for which PBNs were received last month.



PBN Severity

The **PBN Severity** gadget graphically displays the severity levels of the received PBNs. Clicking a bar within the graph takes you to the **Manage PBNs** page which lists the PBNs.

For example, when you click the green bar of the **PBN Severity** gadget (as shown in the following figure), the **Manage PBNs** page displays only the PBNs with Minor severity level that were received.



Service Insight Notices

The **Service Insight Notices** gadget provides the following links:

- EOL product information and announcement: <http://www.juniper.net/alerts/>
- EOS information: <https://www.juniper.net/support/eol/>

Related Documentation

- [Insight Central Overview on page 207](#)
- [Service Insight Domain Overview on page 205](#)

Service Insight Domain Overview

A domain is a logical grouping of objects in Junos Space. A Junos Space administrator creates and manages domains in the Junos Space Network Management Platform. For information about domains, see the *Junos Space Network Management Platform User Guide*.

A device is assigned to a domain in the Junos Space Network Management Platform. When the device is added to Service Now, the device continues to belong to the domain assigned to it in the Junos Space Network Management Platform.

When you access Service Insight, only the EOL Report, PBN Report, and Notification objects, which are assigned to the domain that you are currently in, are visible to you. If you are assigned to more than one domain, you can access those domains and objects in those domains by selecting them from the **Login as *username*** in drop-down list on the banner of the Junos Space GUI. Only the domains to which you are assigned are listed in the list. A super user can access all domains.

Notification objects that you create when you are logged in to a certain domain is assigned to that domain. If needed, you can assign these object to another domain. For information about assigning an object to another domain, see [“Assigning a Service Insight Object to Another Domain” on page 206](#).

Targeted PBN objects, used by objects in all domains, are assigned to the system domain. Objects assigned to the system domain are visible on all the domains and cannot be assigned to another domain. [Table 22 on page 205](#) lists Service Insight objects and their default domains.

Table 22: Service Insight Objects and Their Default Domains

Service Insight Objects	Default Domain	
	Fresh Installation	Migration
<ul style="list-style-type: none"> EOL Reports PBN Reports Notifications 	Domain in which a user is logged	Global domain
<ul style="list-style-type: none"> Targeted PBNs 	System domain	System domain
<ul style="list-style-type: none"> Service Insight Devices 	Domain assigned to the devices in Junos Space Network Management Platform	Domain assigned to the devices in Junos Space Network Management Platform

Assigning a Service Insight Object to Another Domain

If you are assigned to multiple domains, you can assign a Service insight object from the domain that you are currently logged in to another domain to which you are assigned. All objects except objects in the system domain can be assigned to another domain.

To assign a Service Insight object to another domain:

1. From the Service Insight navigation tree, select the object.

The object's inventory landing page appears.

2. On the inventory landing page, select the object that you want to assign to another domain.

3. From the Actions menu, select **Assign object to domain**. Alternatively, right-click the object and select **Assign object to domain**.

The Assign to Domain dialog box appears.

4. Under Assign selected items to domain, select the domain and click **Assign**.

The object is not listed on the object's inventory landing page.

5. To verify that the object is assigned to the correct domain, from the **Login as username** in list, select the domain to which you assigned the object.

The GUI is refreshed.

6. Using the Service Insight navigation tree, open the object's inventory landing page and check whether the object is listed on the page.

Related Documentation

- [Insight Central Overview on page 207](#)
- [Administration Overview on page 71](#)
- *Managing Domains Overview*

CHAPTER 9

Insight Central

- [Insight Central Overview on page 207](#)
- [Exposure Analyzer on page 208](#)
- [Managing EOL Reports on page 213](#)
- [Managing PBN Reports on page 217](#)
- [Managing PBNs on page 220](#)
- [Managing Notifications on page 224](#)

Insight Central Overview

- [Insight Central Overview on page 207](#)

Insight Central Overview

- [Insight Central Overview on page 207](#)

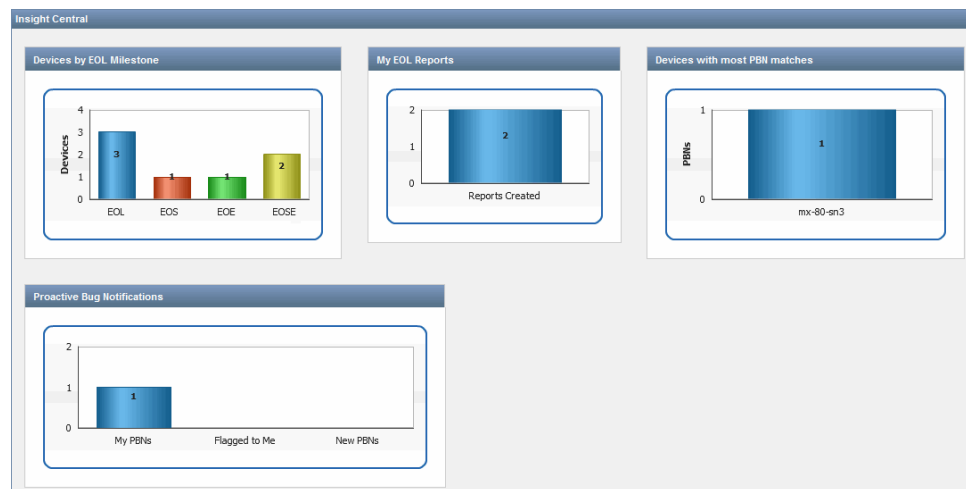
Insight Central Overview

Insight Central is a Service Insight workspace where you can manage devices for which End Of Life (EOL) reports are received, manage the EOL reports and the Proactive Bug Notifications (PBNs). The Exposure Analyzer page within Insight Central displays devices and the available number of EOL parts for these devices, and also displays, for each device, the number of PBNs received. Using the Insight Central workspace, you can also send and manage notifications about EOL and PBN updates to multiple users. You can define the events that trigger a notification, the filters that further specify the trigger events, and also the actions that you want Service Insight to take after the notification is triggered.

To access the Insight Central workspace, you must first enable the Service Insight application. Juniper Care and Juniper Care Plus customers have access to Service Insight. The functionality of Service Insight is dependent on the information sent from Service Now. To enable Service Insight, you must add a valid organization in the Service Now application. See [“Adding an Organization” on page 75](#).

The Insight Central landing page (as shown in [Figure 47 on page 208](#)) graphically displays information about devices and their milestones, EOL reports, PBN reports, the devices with most PBN matches, new PBNs, PBNs owned by you, and the PBNs that are flagged to you.

Figure 47: Insight Central Landing Page



Related Documentation

- [Service Insight Overview on page 200](#)
- [Exposure Analyzer Overview on page 208](#)
- [EOL Reports Overview on page 213](#)
- [PBN Reports Overview on page 217](#)
- [Targeted PBNs Overview on page 220](#)
- [Notifications Overview on page 224](#)

Exposure Analyzer

- [Exposure Analyzer on page 208](#)

Exposure Analyzer

- [Exposure Analyzer Overview on page 208](#)
- [Generating EOL Reports on page 210](#)
- [Generating PBN Reports on page 211](#)
- [Showing Matching PBNs on page 213](#)

Exposure Analyzer Overview

Service Insight lists devices and any End Of Life (EOL) reports or Proactive Bug Notifications (PBNs) that are received for the devices (see [Figure 48 on page 209](#)). The Quick View area of Exposure Analyzer page displays the devices (showing details such as number of EOL parts and number of matching PBNs) with specific icons. [Table 23 on page 209](#) describes these icons. [Table 24 on page 210](#) describes the fields on the Exposure Analyzer page and the Device Details page.

Using Exposure Analyzer, you can generate EOL reports and PBN reports for a particular device. The reports are exported in Excel format. An EOL report includes the following

items: number of devices with End Of Life announce parts, Last Order Dates parts, End of HW Engineering parts, End of SW Engineering parts, and End Of Support parts for the devices that you select. A PBN report includes the following items: Device Name, Device Serial Number, Product, Junos Version, Device Group, Connected Member, Organization, PBN Title, Juniper ID, PBN Description, PBN Customer Impact, PBN Work Around, and PBN URL. EOL reports and PBN reports are exported in Excel format.

Service Insight uses two timers, one that runs every midnight, and another that runs every hour. The hourly timer initiates the processing of pending EOL requests. This timer schedules when JSS sends these requests to the corresponding devices. When large number of devices are added to Service Insight, JSS sends these requests in batches. The timer that runs every midnight updates the EOL and PBN data by sending requests to JSS and processing the responses that are received from JSS. This timer also initiates the synchronization process between Service Now and Service Insight which enables Service Insight to display the changes that were made to devices in Service Now. When you execute device related actions in Service Now while either one of these timers is running, Service Insight takes an hour to display the changes corresponding to these actions on the **Exposure Analyzer** page.

Figure 48: Exposure Analyzer Page

Organization	Connected Member	Device Group	Name	Last Update	EOL Parts	PBN Matches
JCare-Plus		Default for JCare-Plus	device1		0	0
JCare-Plus		Default for JCare-Plus	device2	Oct 15, 2013 5:33:54 PM IST	0	1
JCare-Plus		Default for JCare-Plus	device3		0	0
JCare-Plus		Default for JCare-Plus	device4	Sep 25, 2013 2:03:16 PM IST	0	0
JCare-Plus		Default for JCare-Plus	device5	Oct 24, 2013 12:38:09 PM IST	2	0
JCare-Plus		Default for JCare-Plus	device6	Oct 24, 2013 12:38:09 PM IST	6	0
JCare-Plus		Default for JCare-Plus	device7	Oct 24, 2013 12:38:09 PM IST	19	0

Table 23 on page 209 describes the icons on the exposure analyzer page.

Table 23: Exposure Analyzer Page Icon Descriptions



Icon	Description
	An EOL report is received for the device
	A PBN is received for the device.

Table 24 on page 210 describes the fields on the Exposure Analyzer page and the Device Details dialog box.

Table 24: Device Details from the Exposure Analyzer Page

Field	Description
Name	The device hostname.
Serial Number	Serial number of the device chassis.
IP Address	IP address of the device.
Product	Model number of the device.
Organization	Service Now organization to which the device belongs.
Device Group	Service Now device group to which the device belongs.
Connected Member	Customer connected to the device.
Connection Status	Connection status of the device in Junos Space. <ul style="list-style-type: none"> • up—device is connected to Junos Space. • down—device is not connected to Junos Space.
EOL status	EOL information of the device.
EOL Parts	The parts of the device identified for EOL.
Matching PBNs	Number of PBNs received for the device.
Last updated	Latest date and time when the device connection was updated.

You can perform the following tasks from the **Exposure Analyzer** page:

- [“Generating EOL Reports” on page 210.](#)
- [Generating PBN Reports on page 211](#)
- [“Showing Matching PBNs” on page 213.](#)

Related Documentation

- [Targeted PBNs Overview on page 220](#)
- [Notifications Overview on page 224](#)

Generating EOL Reports

Devices with End Of Life (EOL) information are identified and displayed on the Exposure Analyzer page. Using Service Insight, you can generate EOL reports for these devices in an Excel file. EOL reports provide information such as the number of devices with EOL parts, EOL announce date, number of EOL announce parts, End Of Engineering SW date, number of End Of Engineering SW parts, End Of Engineering HW date, number of End Of Engineering HW parts, End Of Support date, number of End Of Support parts, top-level

assembly parts, circuit assembly parts, PSN numbers, and replacement numbers. You can also schedule a time for generating the EOL reports.

To generate EOL reports:

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 the EOL report.

3. Select **Generate EOL Reports** either from the **Actions** list or the right-click menu. The **Generate EOL Report** dialog box appears.

4. Enter a name for the EOL report.

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

5. Enter the e-mail address of the user to whom the EOL report must be sent.

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

6. 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.

7. 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 and for all the other successive reports, the report name is appended with timestamp.

8. Click **Submit**.

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

9. Click the job ID link.

The Jobs page displays the details of the generated EOL report. The report includes the schedule for the generation of successive PBN reports if the Repeat option is configured.

10. If you want to cancel the scheduled job for generating the next EOL report, select **Cancel Job** either from the **Actions** list or the right-click menu.

Related Documentation

- [EOL Reports Overview on page 213](#)

Generating PBN Reports

Service Insight provides Proactive Bug Notifications (PBNs) as a proactive measure to alert about known issues that can impact the devices in the network. You can also set the scheduling time for generating PBN reports such that they are generated on a set schedule. Devices with PBN information are identified and displayed on the Exposure Analyzer page. Using Service Insight, you can generate PBN reports for these devices in an Excel file. A PBN report includes the following items: Device Name, Device Serial Number, Product, Junos Version, Device Group, Connected Member, Organization, PBN

Title, Juniper ID, PBN Description, PBN Customer Impact, PBN Work Around, and PBN URL.

To generate PBN reports:

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 the PBN report.
3. Select **Generate PBN Reports** from either the **Actions** list or the right-click menu. The **Generate PBN Report** dialog box appears.

4. Enter a name for the PBN report.

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

5. Select **All devices** if you want the PBN report to be generated for all the devices or select **Selected devices shown below** if you want the PBN reports to be generated for only the selected devices in the page.
6. 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.

7. 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.
8. 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 and for all the other successive reports, the report name is appended with timestamp.

9. Click **Submit** after selecting the required options. The Job Information dialog box displays a job ID link for the generated report.

10. Click the job ID link.

The Jobs page displays the details of the generated PBN report. The report includes the schedule for the generation of successive PBN reports if the Repeat option is configured.

The generated report can be saved or downloaded as an Excel sheet. The saved report can be viewed in PBN reports page. If you do not want to save the report in Service Insight, select **Do not save this report on Service Insight** at the top of the page.

11. If you want to cancel the scheduled job for generating the next PBN report, select **Cancel Job** either from the **Actions** list or the right-click menu.

Related Documentation • [PBN Reports Overview on page 217](#)

Showing Matching PBNs

Using Service Insight, you can view the list of PBNs that are associated with one device or up to ten devices simultaneously.

To view PBNs for a device:

1. From the Service Insight navigation tree, select **Insight Central > Exposure Analyzer**. The list of devices appears.
2. Select the devices for which PBNs are to be viewed. You can select up to ten devices.
3. Right-click your selection or use the **Actions** list and select **Show Matching PBNs**. The **Manage PBNs** page displays the list of PBNs that are associated with the device that you selected.

- Related Documentation**
- [Exposure Analyzer Overview on page 208](#)
 - [Targeted PBNs Overview on page 220](#)
 - [Notifications Overview on page 224](#)

Managing EOL Reports

- [Managing EOL Reports on page 213](#)

Managing EOL Reports

- [EOL Reports Overview on page 213](#)
- [Exporting EOL Reports on page 214](#)
- [Deleting EOL Reports on page 215](#)
- [Regenerating EOL Reports on page 215](#)

EOL Reports Overview

The **EOL Reports** page displays the EOL reports that you generate as shown in [Figure 49 on page 213](#). Using this page, you can export the existing EOL reports to an Excel file, regenerate the report to get the latest information, and delete the EOL reports from the Service Insight database. To filter the devices that have EOL parts, double-click an EOL report to display its detailed summary view, and click the link at the bottom of the displayed dialog box.

Figure 49: EOL Reports Page View

Name	Date created	Last ran on	Created by	Devices selected	Devices with EOL parts	Number of EOL parts
TestEOL	Oct 25, 2013 3:12:28 PM IST	Oct 25, 2013 3:12:28 PM IST	super	7	3	27
EOL123	Oct 4, 2013 3:10:00 PM IST	Oct 4, 2013 3:10:00 PM IST	super	4	1	5

[Table 25 on page 214](#) describes the fields on the **EOL Reports** page and the **EOL Report Detail** dialog box.

Table 25: EOL Reports Page and EOL Report Detail Dialog Box Fields Description

Field	Description
Name	Name of the EOL report.
Date created	Date and time when the EOL report was created.
Last Ran On	Date and time when the EOL report was last run.
Created by	Name of the user who created the EOL report.
Devices selected	Number of devices that were selected to generate the EOL report.
Devices with EOL parts	Number of devices with parts for which EOL has been announced or is in progress.
End Of Life Announce Parts	Number of devices with parts whose EOL dates have been announced.
Last Order Dates Parts	Number of devices with parts that have exceeded the last order date. These parts can no longer be ordered from Juniper Networks or a Juniper Networks partner.
End of HW Engineering parts	Number of devices with hardware that is no longer available for order or RMA.
End of SW Engineering parts	Number of devices with software or firmware that is no longer available from Juniper Networks.
End Of Support Parts	Number of devices with parts that have exceeded their End Of Support date. Technical support is no longer available for these parts.
Link to the list of devices with EOL parts.	Link to the Exposure Analyzer page which displays only the devices with EOL parts.

You can perform the following tasks using the **EOL Reports** page:

- [Exporting EOL Reports on page 214](#)
- [Regenerating EOL Reports on page 215](#)
- [Deleting EOL Reports on page 215](#)

Related Documentation

[Generating EOL Reports on page 210](#)

Exporting EOL Reports

You can export the information in an EOL report to an Excel file and save it on your local file system. The EOL report includes information such as the device EOL announce date, End Of Engineering SW date, End Of Engineering HW date, End Of Service date, top-level assembly parts, circuit assembly parts, PSN numbers, EOL model numbers, and replacement numbers.

To export EOL reports:

1. From the Service Insight navigation tree, select **Insight Central > EOL Reports**. The **EOL Reports** page appears.
2. Select the report that you want to export to the Excel file.
3. Select **Export EOL Reports** from either the **Actions** list or the right-click menu. The **Export EOL Report** appears.
4. Click the **Click here to download EOL reports** link and save the file to your local file system.

**Related
Documentation**

- [Generating EOL Reports on page 210](#)
- [EOL Reports Overview on page 213](#)

Deleting EOL Reports

You can delete multiple EOL reports from the EOL Reports page. Deleted EOL reports cannot be recovered.

To delete EOL reports:

1. From the Service Insight navigation tree, select **Insight Central > EOL Reports**. The EOL reports are displayed.
2. Select one or more EOL reports that you want to delete.
3. Select **Delete** either from the **Actions** list or the right-click menu. The **Delete EOL Reports** dialog box appears and displays the names of the selected EOL reports.
4. Click **Delete**. The selected EOL reports are deleted from the database and are no longer displayed on the **EOL Reports** page.

**Related
Documentation**

- [Generating EOL Reports on page 210](#)
- [EOL Reports Overview on page 213](#)

Regenerating EOL Reports

Using Service Insight, you can regenerate an EOL report to get the latest EOL information.

To regenerate EOL reports:

1. From the Service Insight navigation tree, select **Insight Central > EOL Reports**. The EOL Reports page is displayed.
2. Select the EOL report that you want to regenerate.
3. Select **Regenerate EOL Reports** from either the **Actions** list or the right-click menu.

The **Regenerate EOL Report** dialog box displays the name of the EOL report, the device name with which the EOL report is associated, and the e-mail addresses specified. See [Figure 50 on page 216](#).

Figure 50: Regenerate EOL Report Dialog Box

Regenerate EOL Report

EOL Report name:
EOL123

Create EOL Report for:

Device Name	EOL Data Available
device1	Yes
device2	Yes
device3	Yes
device4	No

Send Email To:

Add Email **Delete**

Email List

- ☐ user@example.com

☒ **Schedule at a later time**

Date and time:

11/05/13 3:32 PM IST

Submit **Cancel**

- (Optional) To modify the list of e-mail addresses of users to whom the EOL report must be sent, use the **Add Email** and **Delete** buttons.
- (Optional) To schedule a time for regenerating the report, select the **Schedule at a later time** check box and specify the date and time when you want the EOL report to be regenerated.
- Click **Submit**.
The Job Information dialog box displays a Job ID link. Click this link to view the status of this action on the **Jobs** page.

Related Documentation

- [Generating EOL Reports on page 210](#)
- [EOL Reports Overview on page 213](#)

Managing PBN Reports

- [PBN Reports Overview on page 217](#)
- [Exporting PBN Reports on page 218](#)
- [Deleting PBN Reports on page 218](#)
- [Regenerating PBN Reports on page 218](#)

PBN Reports Overview

The **PBN Reports** page displays the PBN reports that you generate as shown in Figure . Using this page, you can export the existing PBN reports to an Excel file, regenerate them to get the latest information, and delete them from the Service Insight database. To filter the devices that have PBN data, double-click a PBN report to display its detailed summary view, and click the link at the bottom of the displayed dialog box. See [Figure 51 on page 217](#).

Figure 51: PBN Reports page

Name	Date created	Last ran on	Created by	Devices selected	Devices Matching PBNs
PBN321	Oct 4, 2013 3:27:07 PM IST	Oct 4, 2013 3:27:07 PM IST	super	3	3

[Table 26 on page 217](#) describes the fields on the Manage PBN Reports page and the PBN Report Detail dialog box.

Table 26: PBN Reports Page and PBN Report Detail Dialog Box Fields Description

Field	Description
Name	Name of the PBN report.
Date Created	Date and time when the PBN report was created.
Last Ran On	Date and time when the PBN report was last run.
Created By	Name of the user who created the PBN report.
Devices Selected	Number of devices that were selected to generate the PBN report.
Device Name	Name of the device.
Devices with PBNs	Number of devices for which PBNs have been received.

You can perform the following tasks using the **PBN Reports** page:

- [Exporting PBN Reports on page 218](#)
- [Regenerating PBN Reports on page 218](#)
- [Deleting PBN Reports on page 218](#)

- Related Documentation**
- [Generating PBN Reports on page 211](#)

Exporting PBN Reports

You can export the information in a PBN report to an Excel file and save it on your local file system. The PBN report includes information such as the Device Name, Device Serial Number, Product, Junos Version, Device Group, Connected Member, Organization, PBN Title, Juniper ID, PBN Description, PBN Customer Impact, PBN Work Around, PBN URL.

To export PBN reports:

1. From the Service Insight navigation tree, select **Insight Central > PBN Reports**. The **PBN Reports** page appears.
2. Select the report that you want to export to an Excel file.
3. Select **Export PBN Reports** from either the **Actions** list or the right-click menu. The **Export PBN Report** dialog box appears.
4. Click the **Click here to download PBN reports** link and save the file to your local file system.

- Related Documentation**
- [Generating PBN Reports on page 211](#)
 - [PBN Reports Overview on page 217](#)

Deleting PBN Reports

You can delete multiple PBN reports from the PBN Reports page. Deleted PBN reports cannot be recovered.

To delete PBN reports:

1. From the Service Insight navigation tree, select **Insight Central > PBN Reports**. The PBN reports are displayed.
2. Select one or more PBN reports that you want to delete.
3. Select **Delete** from the Action list or the right-click menu. The **Delete PBN Reports** dialog box displays the names of the selected PBN reports.
4. Click **Delete**. The selected PBN reports are deleted from the database and are no longer displayed on the **PBN Reports** page.

- Related Documentation**
- [Generating PBN Reports on page 211](#)
 - [PBN Reports Overview on page 217](#)

Regenerating PBN Reports

Using Service Insight, you can regenerate an PBN report to get the latest PBN information.

To regenerate PBN reports:

1. From the Service Insight navigation tree, select **Insight Central > PBN Reports**.

The PBN reports are displayed.

2. Select the PBN report that you want to regenerate.
3. Right-click your selection or use the **Actions** list and Select **Regenerate PBN Reports** from either the **Actions** list of the right-click menu.

The **Regenerate PBN Report** dialog box displays the name of the PBN report, the device name with which the PBN report is associated, and the e-mail addresses specified.

See [Figure 52 on page 219](#).

Figure 52: Regenerate PBN Report Dialog Box

Regenerate PBN Report

PBN Report name:
PBN321

Create PBN Report for:

Device Name	PBN Data Available
device1	No
device2	No
device3	No

Send Email To:

Add Email **Delete**

Email List

- ☐ user@example.com

☐ **Schedule at a later time**

Submit **Cancel**

4. (Optional) To modify the list of e-mail addresses of users to whom the PBN report must be sent, use the **Add Email** and **Delete** buttons.

5. (Optional) To schedule a time for regenerating the report, select the **Schedule at a later time** check box and specify the date and time when you want the PBN report to be regenerated.
6. Click **Submit**.
The Job Information dialog box displays a Job ID link. Click this link to view the status of this action on the **Manage Jobs** page.

Related Documentation

- [Generating PBN Reports on page 211](#)
- [PBN Reports Overview on page 217](#)

Managing PBNs

- [Managing PBNs on page 220](#)

Managing PBNs

- [Targeted PBNs Overview on page 220](#)
- [Scanning PBNs for Impact on page 221](#)
- [Flagging PBNs to Users on page 222](#)
- [Assigning PBN Ownership on page 223](#)
- [Deleting PBNs on page 223](#)
- [E-Mailing PBNs on page 224](#)

Targeted PBNs Overview

Service Insight provides Proactive Bug Notifications (PBNs) as a proactive measure to alert you about known issues that can impact the devices in your network. It is an effective means of communicating the information collected while helping one customer fix issues to another customer who could face similar issues in future.

Using this information, which was collected when issues were reported to Juniper Networks, Service Insight identifies devices on your network with similar conditions. When devices are identified on your network to have the similar configuration as those devices on which issues were found, the PBNs associated with these devices are displayed on the **Manage PBNs** page. These PBNs keep you aware of the possible impacts and also of ways to fix the issue. PBNs also contain workarounds that suggest temporary fixes and instructions that you can follow to protect your network. Service Insight checks for new PBNs and updates the existing PBNs every 24 hours.

Using The **Manage PBNs** page, you can scan PBNs to display only those devices that are impacted by the vulnerabilities described by the selected PBN, flag PBNs to users, assign owners to the PBNs, e-mail the PBNs to users, and delete them. You can also create notifications that will alert users when new PBNs arrive or when a new PBN match is found.

[Table 27 on page 221](#) describes the fields displayed on the **Manage PBNs** page and the PBNs detail summary view.

Table 27: Manage PBNs Page Fields Description

Field	Description
Title	Short description of the issue found.
Issue Date	Date and time when the issue was recorded.
Juniper ID	Unique ID specified by Juniper Networks that is used to identify the PBN.
Resolved In	Date and time when the problem in this PBN was resolved.
Description	Short description of the problem.
Trigger	Conditions that initiated the problem described by the PBN.
Symptom	Conditions that indicate that the problem described by the PBN has occurred.
Work Around	Temporary fix for the problem.
Instructions	Additional information that you can follow.
Relevances	The platforms and device that could be impacted by the problem described by the PBN.
Impact Probability	The probability that the bug would impact the network.
Customer Impact	The impact of the bug on the customer network.
Owner	The user who has been assigned ownership of the PBN using Service Insight.
Flagged to Users	The users who were notified about the PBN using Service Insight.

- Related Documentation**
- [Exposure Analyzer Overview on page 208](#)
 - [Scanning PBNs for Impact on page 221](#)
 - [Assigning PBN Ownership on page 223](#)
 - [Flagging PBNs to Users on page 222](#)
 - [E-Mailing PBNs on page 224](#)

Scanning PBNs for Impact

You can use Service Insight to identify the devices that could be impacted by the vulnerabilities described in a PBN.

To scan PBNs and view the impacted devices:

1. From the **Service Insight** taskbar, select **Insight Central > Targeted PBNs**.

The **Manage PBNs** page displays the list of PBNs.

2. Select the PBN that you want to scan for impact.
3. Right-click your selection or use the **Actions** list and Select **Scan for Impact**
The **Scan for Impact Results** page displays the list of devices that the vulnerabilities described in the selected PBN could impact.
4. Click **Confirm** to scan the PBNs.

The **Job Information** page displays the schedule status of the selected PBNs. To view the details, click the Job ID. The scan details appear on the **Job Management** page.

**Related
Documentation**

- [Exposure Analyzer Overview on page 208](#)
- [Assigning PBN Ownership on page 223](#)

Flagging PBNs to Users

You can flag PBNs to Junos Space users who you think need to keep track of the PBNs or who need to receive them.

To flag a PBN to a user:

1. From the **Service Insight** navigation tree, select **Insight Central > Targeted PBNs**.

The **Manage PBNs** page displays the list of PBNs.

2. Select the PBN that you want to flag to the user.
3. From the **Actions** list or the right-click menu, select **Flag to Users**.

The **Flag to Users** dialog box displays the list of users who have permissions to view, assign ownership, or delete PBNs.

4. Select the users to whom the PBN must be flagged.
5. Select the **Email PBN to Flagged Users** check box to send an e-mail notification to all the newly flagged users. This option is selected by default.
6. Click **Submit**.

The specified users receive notification about the selected PBN.

To verify that the specified users have been notified of the selected PBN, double-click the PBN and view the **Flagged to Users** field of the PBN in the **PBN. Details** dialog box.

**Related
Documentation**

- [Exposure Analyzer Overview on page 208](#)
- [Scanning PBNs for Impact on page 221](#)
- [Assigning PBN Ownership on page 223](#)

Assigning PBN Ownership

You can assign a PBN to a Junos Space user who needs to be notified of the PBN and is responsible for the PBN.

To assign ownership of a PBN:

1. From the Service Insight navigation tree, select **Insight Central > Targeted PBNs**.
The **Manage PBNs** page displays the list of PBNs.
2. Select the PBN to which you want to assign an owner.
3. Right-click your selection or use the **Actions** list, select **Assign Ownership**.
The Assign Ownership dialog box appears
4. Enter the login ID of the user who would own the selected PBN.
5. Select the **Email PBN to Assigned Owner** check box to send an e-mail notification to the assigned owner. This option is selected by default.
6. Click **Submit**.
The selected PBN is assigned to the specified user.
To verify that the selected PBN is assigned to the specified user, double-click the PBN on the **Targeted PBNs** page and view the **Owner** field of the PBN in the **PBN Details** dialog box.

- Related Documentation**
- [Exposure Analyzer Overview on page 208](#)
 - [Scanning PBNs for Impact on page 221](#)

Deleting PBNs

You can delete PBNs that are displayed on the Manage PBNs page.

To delete PBNs:

1. From the Service Insight navigation tree, select **Insight Central > Targeted PBNs**.
The Manage PBNs page displays the list of PBNs.
2. Select the PBNs that you want to delete.
3. Right-click your selection or use the **Actions** list and select **Delete**.
The **Delete PBNs** dialog box displays a list of the selected PBNs.
4. Click **Delete** to confirm.
The selected PBNs are deleted from the Service Insight database and no longer listed in the Targeted PBNs page.

- Related Documentation**
- [Exposure Analyzer Overview on page 208](#)
 - [Scanning PBNs for Impact on page 221](#)
 - [Assigning PBN Ownership on page 223](#)

E-Mailing PBNs

Using Junos Space, you can e-mail PBN details to multiple users.

To e-mail PBN details:

1. From the Service Insight navigation tree, select **Insight Central > Targeted PBNs**. The **Manage PBNs** page displays the list of PBNs.
2. Select the PBN that you want to e-mail to users.
3. Right-click your selection or use the **Actions** list and select **Email**. The **Email PBN Details** dialog box appears.
4. Use the **Add Email** and **Delete** buttons to add and delete e-mail IDs of users to whom the selected PBN details need to be sent. By default, the e-mail ID of the logged-in user is added to the **Send Email To** list of users.
5. (Optional) To schedule a time for e-mailing the selected PBNs, select the **Schedule at a later time** check box and specify the date and time when you want the PBNs to be e-mailed.
6. Click **Submit**.
The selected PBNs are e-mailed to the specified users.

- Related Documentation**
- [Exposure Analyzer Overview on page 208](#)
 - [Scanning PBNs for Impact on page 221](#)
 - [Assigning PBN Ownership on page 223](#)

Managing Notifications

- [Managing Notifications on page 224](#)

Managing Notifications

- [Notifications Overview on page 224](#)
- [Creating and Copying a Notification on page 225](#)
- [Editing the Filters and Actions of a Notification on page 228](#)
- [Enabling and Disabling Notifications on page 228](#)
- [Deleting Notifications on page 229](#)

Notifications Overview

In Service Insight, you can create notifications to alert users when a specific event occurs. You can also specify the actions that Service Insight must take when an event is triggered.

Specify the following parameters when you create a notification:

- **Trigger**—Specify the event that causes Service Insight to send the notification. The types of triggers are:
 - **New EOL Match**—an e-mail notification is sent when an EOL announcement is received and one or more devices are affected by the announcement.
 - **New PBN Arrival**—an e-mail notification is sent when a new PBN is received and matches one or more devices.
 - **New PBN Match**—an e-mail notification is sent when a PBN affects one or more devices.
- **Filters**—Specify additional details about the event that cause Service Insight to send a notification.
- **Actions**—Specify the action (or actions) that must be taken after a specified event is triggered. These events can be filtered by public tags (applied on devices listed on the Exposure Analyzer page), device name, and serial number.

The Notifications page enables you to manage these notifications. This page displays the notifications chronologically by name, owner, status, and trigger. [Table 28 on page 225](#) provides more information about the fields on the **Manage Notifications** page.

Table 28: Manage Notifications Page Fields Description

Field Name	Description	Range/Length
Name	Name of the notification. The notification name must be unique	64 characters
Owner	User name of the user who owns the notification.	Not applicable
Status	Functional status of the notification.	Enabled or Disabled
Trigger Type	Type of the trigger for which the notification is applied.	<ul style="list-style-type: none"> • New EOL Match • New PBN Arrival • New PBN Match

Related Documentation

- [Targeted PBNs Overview on page 220](#)
- [Creating and Copying a Notification on page 225](#)
- [Enabling and Disabling Notifications on page 228](#)

Creating and Copying a Notification

You can specify when you want Service Insight to send notifications, and also the recipients of the notification. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Insight

to take after the event is triggered. Service Insight enables you to create and copy notifications:

- [Creating a Notification on page 226](#)
- [Copying a Notification on page 226](#)

Creating a Notification

To create a notification policy:

1. From the Service Insight navigation tree, select **Insight Central > Notifications > Create Notifications**.
The **Create Notifications** dialog box appears. For descriptions about the fields on this page see [Table 29 on page 226](#).
2. Enter a name for the notification and select a trigger.
3. (Optional) Specify filters, such as the tags included, device name, and serial number. When you select the **New PBN Arrival** or **New PBN Match** trigger, you are allowed to specify two additional filters. These two filters allow you to filter the PBNs based on the words that it has or does not have.
4. Enter the e-mail IDs of the recipients of the notification using the **Add Email** button.
5. Click **Add**.
The notification is created and displayed on the **Notifications** page.

Copying a Notification

To copy a notification:

1. From the Service Insight navigation tree, select **Insight Central > Notifications**.
The **Manage Notifications** page displays the notifications. For descriptions about the fields on this page see [Table 29 on page 226](#).
2. Select the notification whose attributes you want to copy to create another notification.
3. Right-click your selection or use the **Actions** list and select **Copy**.
The **Notifications** dialog box displays the attributes of the selected notification.
4. Make your modifications to the name, applied filters, and the actions. The trigger field cannot be modified. By default, the word Copy is added as a prefix to the name of the notification.
5. Click **Copy**.
The notification is created and listed in the Notifications page.

Table 29: Manage Notifications Page Field Description

Field	Description	Range/Length
Name	Enter the name of the notification.	64 characters

Table 29: Manage Notifications Page Field Description (*continued*)

Field	Description	Range/Length
Trigger Type	Select the type of trigger required to activate the notification. The fields in the Apply Filter section change dynamically according to the trigger type that you select.	<ul style="list-style-type: none"> • New EOL Match • New PBN Arrival • New PBN Match
Apply Filters		
Includes Tag	<p>Select a value from the list that displays the tags that you can specify. Service Insight sends a notification when the specified trigger type contains this tag.</p> <p>When a public tag that is set as a filter level for a notification is deleted, the notification continues to be displayed on the Manage Notifications page with its status changed to Disabled. You are notified of this change when the notification is triggered.</p>	255 characters
Device Name	Enter a value in the Device Name field. Service Insight sends a notification if the name of the device associated with the EOL or PBN that triggered the notification matches the entered value.	255 characters
Serial Number	Enter a value in the Serial Number field. Service Insight sends a notification if the serial number of the device associated with the EOL or PBN that triggered the notification matches the entered value.	255 characters
Has the words	<p>Enter a value in the Has the words field. Service Insight sends a notification if the specified words match the words in the title of the PBN that triggered the notification.</p> <p>This field appears only when you select the New PBN Arrival trigger type.</p>	255 characters
Does not have	<p>Enter a value in the Doesn't have field. Service Insight sends a notification if the specified words do not match any of the words in the title of the PBN that triggered the notification.</p> <p>This field appears only when you select the New PBN Arrival trigger type.</p>	255 characters
Actions		
Send Email to	<p>Specify the e-mail addresses of users who must receive an alert when the notification is triggered and matches the specified filters.</p> <p>To add a new e-mail address to the list, click Add Email. Click the Enter Email Id field to enter the e-mail address. The e-mail address should be in the format user@example.com.</p> <p>To delete an e-mail address from the list, select the e-mail address and click Delete.</p>	65535 characters
Send SNMP Traps to	Specify the destinations where SNMP traps can be sent when the notification is triggered and matches the specified filters. See Adding an SNMP Server.	Not applicable.

Related Documentation

- [Targeted PBNs Overview on page 220](#)
- [Enabling and Disabling Notifications on page 228](#)

Editing the Filters and Actions of a Notification

You can edit notification parameters, such as the applied filters, and the actions that a notification takes.

To edit a notification:

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

The **Manage Notifications** page displays the notifications.

2. Select the notification whose filters and actions you want to edit.
3. Right-click your selection or use the **Actions** list and select **Edit Filters and Actions**.

The **Notifications** dialog box displays the parameters specified for the notification.

4. Make your modifications and click **Save** to save your changes.

To verify that your changes are saved, view the details of the notification on the Notifications page.

Related Documentation

- [Targeted PBNs Overview on page 220](#)
- [Creating and Copying a Notification on page 225](#)
- [Enabling and Disabling Notifications on page 228](#)

Enabling and Disabling Notifications

You can change the functional status of a notification from enabled to disabled, and vice versa. When you create a notification, by default, the notification is in the enabled status where it performs its functions normally. Although the notifications that you disable are inactive and do not perform the specified actions, they are listed on the Manage Notifications page and can be enabled whenever required.

When a public tag that is set as a filter level for a notification is deleted, the notification continues to be displayed on the Manage Notifications page with its status changed to Disabled. You are notified of this change when the notification is triggered.

To enable or disable a notification:

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

The **Manage Notifications** page displays the notifications.

2. Select the notifications whose status you want to modify.
3. Right-click your selection or use the **Actions** list and select **Enable/Disable**.
The Change Notification Status dialog box displays the list of notifications and the changed functional status.

4. Click **Change Status** to confirm.
The status of the selected notifications is modified.

- Related Documentation**
- [Targeted PBNs Overview on page 220](#)
 - [Creating and Copying a Notification on page 225](#)

Deleting Notifications

You can delete multiple notifications from the Manage Notifications page.

To delete notifications:

1. From the Service Insight navigation tree, select **Insight Central > Notifications**. The **Manage Notifications** page displays the notifications.
2. Select the notifications that you want to delete.
3. Right-click your selection or use the **Actions** list and select **Delete**. The **Delete Notification** dialog box displays the list of selected notifications.
4. Click **Delete** to confirm.
The selected notifications are deleted from the Service Insight database. To verify that the selected notifications are deleted, view the notifications displayed on the **Manage Notifications** page.

- Related Documentation**
- [Targeted PBNs Overview on page 220](#)
 - [Creating and Copying a Notification on page 225](#)
 - [Enabling and Disabling Notifications on page 228](#)

CHAPTER 10

JSS Messages Reference

Juniper Support Systems (JSS) uses the Juniper Networks Knowledge Base (KB), engineering expertise, and specialized tools to resolve incident cases. It also uses proactive analysis information that it receives from internal product knowledge, the KB, and the customer's network to provide intelligence updates. JSS receives information from the devices in the network and sends this information, in the form of updates and alerts, to Service Now.

All communication between Service Now and JSS occurs over a secure channel, and each transaction is authenticated and verified by JSS.

This topic describes JSS event messages along with the Juniper Networks recommended course of action for each event. For warnings with no listed actions, the message is informational only.

LIC-1001

System Log Message	Current date is within 60 days beyond expiry. Requests still processed. SKU: xxx has expired
Description	Even though the current date is less than 60 days after the license expired, requests are still being processed.
Type	Warning
Action	Contact Juniper Networks or a Juniper Networks Partner for license renewal.

LIC-1098

System Log Message	SKU: xxx has expired
Description	The current date is more than 60 days after the license expired. Requests will not be processed.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner for license renewal.

LIC-1099

System Log Message	Service license does not exist.
---------------------------	---------------------------------

Description	The service license does not exist.
Action	Contact Juniper Networks or a Juniper Networks Partner for the appropriate license.

LIC-2000

System Log Message	Purchased Capacity Exceeded. Additional capacity SKU xxx required
Description	The class usage of the current product is between 101 and 150 percent of the purchased capacity. Requests are still being processed.
Type	Warning
Action	Contact Juniper Networks or a Juniper Networks Partner for capacity increments.

LIC-2099

System Log Message	Purchased capacity exceeded. Additional capacity SKU xxx required
Description	The class usage of the current product has exceeded 150 percent of the purchased capacity. No more requests can be processed.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner to increase licenses.

LIC-3000

System Log Message	Non-licensable product.
Description	The product is non-licensable.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner for assistance.

LIC-4000

System Log Message	Organization doesn't have JTS Contract. Base Fee SKU [SVC or PAR]-[1-4]-BASE-[R] with BASE or PRO Service level required. Request not processed.
Description	The request was not processed because the organization does not have a JTS contract. You need to have a Base Fee SKU [SVC or PAR]-[1-4]-BASE-[R] with a BASE or PRO Service level.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner to obtain the license.

LIC-4001

System Log Message	Organization's JTS Contract is within 60 days beyond expiry. Request is accepted. Please renew your licenses
Description	The current date is less than 60 days after the organization's JTS contract expired. The request is still accepted but you are asked to renew your licenses.
Type	Warning
Action	Contact Juniper Networks or a Juniper Networks Partner license renewal.

LIC-4002

System Log Message	Organization's JTS Contract is over 60 days beyond expiry. Request is rejected. Base Fee SKU: "xxx" has expired.
Description	The current date is more than 60 days after the organization's JTS contract expired. The request is not accepted. Please renew your licenses.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner for license renewal

LIC-4003

System Log Message	Device not covered under JTS Contract but request is accepted
Description	The request is accepted even though the device is not covered by the JTS contract.
Type	Warning
Action	Contact Juniper Networks or a Juniper Networks Partner for more information.

LIC-4004

System Log Message	Device doesn't have appropriate Service Contract level, but request to open case is accepted.
Description	Even though the service doesn't have the appropriate Service Contract level, the request to open a case is accepted.
Type	Warning
Action	Contact Juniper Networks or a Juniper Networks Partner to add the device to an appropriate Service Contract.

LIC-4005

System Log Message	Device doesn't have JTS Contract, request is rejected. Device SKU: [SVC or PAR]-[1-4]-[SvcType]-[ProdType] required.
---------------------------	--

Description The request is rejected because the device does not have a JTS contract. You need to have a Device SKU: [SVC or PAR]-[1-4]-[SvcType]-[ProdType].

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner for the contract.

LIC-4006

System Log Message Service license does not exist to process PRO operation. Request not processed.

Description The PRO operation request was not processed because the appropriate service license does not exist.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner for the appropriate license.

LIC-4007

System Log Message Partner Model SKU Type is not present for this contract. Request not processed.

Description The request was not processed because the Partner Model SKU type was not present for this contract.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner for the appropriate license.

LIC-4008

System Log Message Partner Model SKU Type is within 60 days beyond expiry. Request is accepted.

Description The request was accepted because the Partner Model SKU Type was within 60 days after its expiration date.

Type Warning

Action Contact Juniper Networks or a Juniper Networks Partner for license renewal.

LIC-4009

System Log Message Organization doesn't have JCare Plus License, request is rejected

Description The request was rejected because the organization did not have JCare Plus License

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner for the appropriate license.

LIC-4010

System Log Message Organization JCare Plus License is within 60 days beyond expiry. Request is accepted.

Description The request was accepted because the Organization JCare Plus License was within 60 days after its expiration date.

Type Warning

Action Contact Juniper Networks or a Juniper Networks Partner for license renewal.

LIC_4011

System Log Message JCare Plus license does not exist SVC-JCP/PAR-JCP license required for processing PBN related information

Description The JCare Plus license does not exist. You need a SVC-JCP/PAR-JCP license to process PBN-related information.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner for the appropriate license.

PVS-1000

System Log Message Undefined service name

Description The service name was not defined.

Type Error

Action Contact your system administrator.

PVS-1001

System Log Message Undefined service method

Description The service method was not defined.

Type Error

Action Contact your system administrator.

PVS-1002

System Log Message Invalid domain value. In the case a value not within a restricted set is passed in.

Description The domain value was not valid because it was not within the restricted set.

Type Error

Action Contact your system administrator.

PVS-1006

System Log Message ClientVersion is required to process the Request

Description A ClientVersion is required to process the request.

Type Error

Action Contact your system administrator.

PVS-1007

System Log Message Unable to process the request For ClientVersion below 4.x

Description Requests cannot be processed for ClientVersions earlier than 4.x.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner.

PVS-1008

System Log Message SiteId is Not Asscoiated to the User

Description The site ID is not associated with the user.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner.

PVS-1009

System Log Message SecondarySiteId is Not Associated to the User

Description The secondary site ID is not associated with the user.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner.

PVS-1010

System Log Message No primarySite is associated to the user

Description No primary site is associated with the user.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner.

PVS-1011

System Log Message No Contract's exist for this Serial Num

Description No contracts exist for this serial number.

Type Warning

PVS-1100

System Log Message	Payload contents not compatible with service method
Description	The payload contents are not compatible with the service method.
Type	Error
Action	Contact your system administrator.

PVS-1200

System Log Message	Record not found
Description	The record not found.
Type	Error
Action	Contact your system administrator.

PVS-1201

System Log Message	Errors encountered retrieving case status information, see payload for details
Description	Errors were encountered while retrieving case status information, see the payload for more details.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1202

System Log Message	Alert not found
Description	The alert not found.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1203

System Log Message	Category not found
Description	The category not found.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1204

System Log Message	Credentials not authenticated or authorized to access CRM
Description	Credentials are not authenticated or authorized to access the CRM.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner for username/password authentication.

PVS-1205

System Log Message	Number of files sent does not match < TotalFiles >
Description	The number of files sent does not match the < TotalFiles > value.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1207

System Log Message	Unable to persist request message
Description	Unable to persist request message.
Type	Error
Action	Contact your system administrator.

PVS-1210

System Log Message	Duplicate create case message found
Description	A duplicate create case message was found.
Type	Warning

PVS-1213

System Log Message	CreateCaseRequest release format invalid, expecting [major].[minor]
Description	The CreateCaseRequest release format was invalid, The format was expected to be [major].[minor].
Type	Error
Action	Contact your system administrator.

PVS-1214

System Log Message	CreateCaseRequest release data type invalid, [major] and [minor] must be numeric
---------------------------	--

Description	The CreateCaseRequest release data type was invalid. The [major] and [minor] values must be numbers.
Type	Error
Action	Contact your system administrator.

PVS-1215

System Log Message	CreateCaseRequest version format invalid, expecting [release-category][build-number]
Description	The CreateCaseRequest version format is invalid. The expected format is [release-category][build-number].
Type	Error
Action	Contact your system administrator.

PVS-1216

System Log Message	CreateCaseRequest version data type invalid, [release-category] must be 'R', 'B', or 'I', [build-number] must be numeric
Description	The CreateCaseRequest version data type is invalid, the [release-category] must be 'R', 'B', or 'I'; and the [build-number] value must be a number.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1223

System Log Message	No organization associated with Site.
Description	No organization was associated with the site.
Type	Error
Action	Contact your system administrator.

PVS-1226

System Log Message	No recent iJMB available
Description	No recent iJMB is available.
Type	Warning
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1227

System Log Message	No EOL records found
---------------------------	----------------------

Description	No EOL records were found.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS_1230

System Log Message	Inform Id does not exist in JSS
Description	Inform ID does not exist in JSS.
Type	Error
Action	Contact Juniper Networks or a Juniper Networks Partner.

PVS-1231

System Log Message	No association found in PVS for Inform ID and the site ID. Please submit the correct inform id to retrieve the details
Description	No association was found in PVS for the Inform ID and the site ID. Please submit the correct inform ID to retrieve the details.
Type	Warning
Action	Contact your system administrator.

PVS-1232

System Log Message	iJMB message already received within last 24 hours.
Description	The iJMB message was already received within last 24 hours.
Type	Warning

PVS-8000

System Log Message	Unable to connect to PvsDB
Description	Unable to connect to PvsDB.
Type	Warning
Action	None. You might experience a delay in connecting to Juniper Networks.

PVS-8001

System Log Message	Unable to connect to CRM
Description	Unable to connect to CRM.
Type	Warning

Action None. You might experience a delay in a case being opened.

PVS-8002

System Log Message Unable to connect to Alerting System

Description Unable to connect to the alerting system.

Type Warning

PVS-8006

System Log Message ESBContracts service is not responding.Please retry after 24 hours

Description The ESBContracts service is not responding. Please wait 24 hours and then retry.

Type Warning

PVS-9000

System Log Message Error uploading file

Description An error occurred in uploading the file.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner.

PVS-9999

System Log Message Internal PvS error

Description An internal PvS error occurred.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner.

SEC-1000

System Log Message Authentication and/or Authorization of credentials failed

Description Authentication and/or authorization of credentials failed.

Type Error

Action Contact Juniper Networks or a Juniper Networks Partner for username/password authentication.

SEV-0001

System Log Message Request failed completely

Description The request failed completely.

Type	Error
Action	Contact your system administrator.

SEV-0002

System Log Message	Request succeeded with warnings
Description	The request succeeded with warnings.
Type	Warning

SEV-0003

System Log Message	Request succeeded with information
Description	The request succeeded with information.
Type	Info

VLD-1000

System Log Message	XML validation error
Description	An XML validation error occurred.
Type	Error
Action	Contact your system administrator.

VLD-2000

System Log Message	Malformed XML document
Description	A malformed XML document was encountered.
Type	Error
Action	Contact your system administrator.

PART 3

Index

- [Index on page 245](#)

Index

A

adding devices.....	90
AI-Script	
install.....	91
remove.....	94
AI-Scripts	
downloading i3ninstall packages.....	27
install location on device hard disk.....	29
install package versioning.....	28

C

collect	
RSI output.....	100
conventions	
notice icons.....	xv
copying a notification.....	226
creating a notification.....	226
customer support.....	xvi
contacting JTAC.....	xvi

D

dashboard overview	
Dashboard Gadgets.....	46
Service Now Workspaces.....	45
deleting	
device.....	105
device group.....	85
iJMB.....	182
incident.....	164
information message.....	177
notification policy.....	194
organization.....	79
device	
associate with device group.....	105
device group	
create.....	83
modify.....	85
disabling a notification.....	228
documentation	
comments on.....	xvi

E

enabling a notification.....	228
end-customer mode.....	42
EOL reports	
deleting.....	215
exporting.....	214
overview.....	213
regenerating.....	215
export device data	
CSV/Excel.....	94
export iJMB	
html.....	181
export inventory information	
CSV/Excel.....	95
exposure analyzer overview.....	208

G

generating eol reports.....	210
generating on demand incidents.....	96
generating pbn reports.....	211
global settings	
global.....	123
proxy server.....	132
snmp server	
add	129
edit/delete.....	131

I

incident	
assigning owner.....	160
export to Excel.....	163
flagging.....	161
submitting.....	165
information message	
assign connected member.....	178
assign owner.....	175
flagging.....	176
insight central overview.....	207

J

JMB error.....	184
----------------	-----

M

managing SNMP Traps.....	131
manuals	
comments on.....	xvi
mode.....	42

N

notice icons.....	xv
notification policy	
create.....	187
enable/disable.....	194
notifications	
deleting.....	229
editing filters and actions.....	228
overview.....	224

O

online, offline mode.....	42
organization	
add.....	75
modify.....	79
run in test mode.....	82
test connection to JSS.....	80
overview	
administration.....	71
AI-Scripts.....	21
device groups.....	83, 86
device snapshots.....	180
EOL reports.....	213
exposure analyzer	208
Incidents.....	158
insight central.....	207
messages.....	175
notifications.....	186, 224
organization.....	73
Service Automation.....	19
Service Central	155
service insight.....	200
service insight dashboard.....	202
targeted PBNs.....	220

P

PBN reports	
deleting.....	218
regenerating.....	218
PBNs	
deleting.....	223
e-mailing.....	224
flagging to users.....	222
overview.....	220
scanning for impact.....	221
show matching PBNs.....	213

S

scan iJMB for ipact.....	177
--------------------------	-----

script bundle	
add.....	121
delete.....	122
service insight	
dashboard gadgets.....	202
dashboard overview.....	202
overview.....	200
Service Now Overview.....	34
support, technical	See technical support

T

technical support	
contacting JTAC.....	xvi

U

user roles.....	51
-----------------	----

V

view	
case in Case Manager.....	171
incident details	169
JMB details.....	182
viewing exposure.....	96