



Service Automation

User Guide

Release

15.1



Modified: 2016-06-23

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 15.1

Copyright © 2016, Juniper Networks, Inc.

All rights reserved.

Revision History

August 2014—Service Automation User Guide, Release 14.1

March 2015—Updated the Adding an Organization topic for PR 1072229.

August 2015—Service Automation User Guide, Release 15.1 Beta Release

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	xvii
	Documentation and Release Notes	xvii
	Documentation Conventions	xvii
	Documentation Feedback	xviii
	Requesting Technical Support	xviii
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xix
Chapter 1	Service Automation Overview	21
	Service Automation Overview	21
Part 1	AI-Scripts	
Chapter 2	AI-Scripts Overview	27
	AI-Scripts Overview	27
	Working Modes of AI-Scripts	27
	Events Detected by AI-Scripts	28
	Types of JMBs	28
	JMB Contents	29
	Logs	34
Chapter 3	Installing AI-Scripts	37
	Downloading AI-Scripts Install Packages and Release Notes	37
	AI-Scripts Install Package Versioning	38
	AI-Scripts Install Locations on Devices	39
	Automatically Installing AI-Scripts Bundles	39
	Manually Installing AI-Scripts on Devices	39

Part 2	Junos Space Service Now	
Chapter 4	Service Now Overview	47
	Service Now Overview	48
	Junos Space Service Now Overview	48
	Service Now Domain	50
	Assigning a Service Now Object to Another Domain	52
	Installing, Upgrading, and Uninstalling Junos Space Service Now and Junos	
	Space Service Insight Applications	53
	Uploading a Service Now Image File to Junos Space server	53
	Installing Junos Space Service Now and Junos Space Service Insight	54
	Upgrading Junos Space Service Now and Junos Space Service Insight	56
	Uninstalling Junos Space Service Now and Junos Space Service Insight	57
	Service Now MIBs	57
	Service Now MIBs	58
	Service Now Modes	58
	Junos Space Service Now Modes	59
	Service Now Dashboard and Workspaces Overview	62
	Service Now Dashboard Overview	63
	Service Now Workspaces	63
	Dashboard Gadgets	64
	Service Now Inventory Pages	66
	Filtering Inventory Pages on Service Now and Service Insight	66
	User Roles	69
	Junos Space Service Now User Roles	69
Chapter 5	Using the Service Now Getting Started Assistant	73
	Service Now Getting Started Assistant Usage Overview	73
	Service Now Getting Started Assistant Usage Overview	73
Chapter 6	Trouble Ticket APIs Supported by Service Now	75
	Trouble Ticket APIs Overview	75
	Profiles Used by Service Now	76
	Setting up Java Based Web Service Client	76
	Accessing a Web Service	82
	Trouble Ticket APIs Supported by Service Now	83
	Error Messages Displayed by OSS/J Client	84
	Trouble Ticket Attributes Supported by Service Now	86
	Trouble Ticket Events Supported by Service Now	88
Chapter 7	Administration	91
	Administration Overview	91
	Organizations	92
	Organizations Overview	93
	Creating Organizations	95
	Adding an Organization to Service Now	95
	Adding an End Customer to Service Now Configured in Partner Proxy	
	Mode	98
	Modifying Organization Parameters	100
	Deleting an Organization	101

Testing the Connection to JSS	102
Viewing Messages Assigned to an End Customer	103
Running an Organization in Test Mode	103
Updating Core File Upload Configuration for an End Customer	104
Device Groups	104
Device Groups Overview	105
Creating a Device Group	105
Modifying a Device Group	107
Deleting a Device Group	107
Service Now Devices	108
Junos Space Service Now Devices Overview	108
Adding Devices to Junos Space Service Now	114
Installing an Event Profile on a Device by Using Service Now	114
Uninstalling an Event Profile from a Device	117
Exporting Device Data in CSV and Excel Formats	119
Exporting Inventory Information in CSV Format	119
Viewing Exposure to Known Issues	120
Generating an On-Demand Incident	121
Collecting RSI and System Log Files	124
Requesting an RMA Incident on Service Now	127
Moving a Device to Maintenance Mode	130
Deleting a Device from Junos Space Service Now	131
Associating Devices with a Device Group	132
Assigning an Auto Submit Policy to a Device	133
Viewing Incidents	134
Verifying the Connection Between a Device and the FTP Server	135
Service Now End Customer–Partner Communication Overview	135
Generating CSR by Service Now Partner	136
Obtaining Signature of a Certificate Authority	138
Uploading the Certificate to Service Now Partner	139
Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate	139
Obtaining SSL Certificate of the Service Now Partner	139
Installing the SSL Certificate on a Service Now End Customer	140
BIOS Validation	141
BIOS Validation Overview	141
Configuring BIOS Validation for Verifying BIOS Integrity of a Device	145
Product Health Data Collection	147
Product Health Data Collection Overview	147
Viewing Product Health Data Files Collected from a Device	149
Product Health Data Collection Configuration Overview	153
Associated Actions	154
Configuring Product Health Data Collection on a Device	155
Configuring PHDC by Using the Product Health Data Collection Task	155
Configuring PHDC by Using the Service Now Devices Task	157
Modifying a Product Health Data Collection Configuration	160
Rescheduling a Product Health Data Collection Configuration	163
Retrying Collecting Product Health Data from a Device	164

Disabling Product Health Data Collection on a Device	165
Enabling Product Health Data Collection on a Device	166
Aborting a Product Health Data Collection Configuration	167
Exporting Product Health Data Information to an Excel File	168
Exporting Information about Devices on which PHDC is configured . . .	169
Exporting Data about PHD Files Collected from a Device	171
Deleting Product Health Data Files Collected from a Device	173
Deleting a Product Health Data Collection Configuration from Service Now	175
Event Profiles and AI-Scripts	176
Event Profiles Overview	177
Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview	178
Associated Actions	181
Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview	182
Adding an Event Profile to Junos Space Service Now	185
Cloning an Event Profile	189
Importing Event Profiles into Junos Space Service Now in XML Format . . .	191
Exporting Event Profiles from Junos Space Service Now in XML Format . .	192
Deleting Event Profiles from Junos Space Service Now	194
Viewing an Event Profile	195
Pushing an Event Profile to Devices	195
Displaying Devices Associated with an Event Profile	198
Setting an Event Profile as the Default Event Profile in Junos Space Service Now	198
Exporting Events Data in Excel Format	199
Adding a Script Bundle to Junos Space Service Now	200
Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now	200
Deleting a Script Bundle from Junos Space Service Now	201
Global Settings	202
Configuring Global Settings	202
Adding an SNMP Configuration to Service Now	204
Editing and Deleting an SNMP Configuration	206
Managing SNMP Traps	207
Viewing Proxy Server Settings Configured on the Junos Space Platform . .	207
Uploading Core Files Generated for Events	208
Auto Submit Policy	210
Auto Submit Policy Overview	210
Creating an Auto Submit Policy	211
Modifying an Auto Submit Policy	215
Deleting Auto Submit Policies from Service Now	216
Exporting an Incidents Report	216
Changing the Status of Auto Submit Policies	217
Changing the Dampening Status of an Auto Submit Policy	218

	Address Group	219
	Address Group Overview	220
	Creating an Address Group	220
	Modifying an Address Group	221
	Deleting Address Groups	221
	Associating Devices with an Address Group From the Address Groups Page	222
	Associating Devices with an Address Group From the Organizations Page	224
	Associating Devices with an Address Group from the Device Groups Page	225
	Associating Devices with an Address Group from the Service Now Devices Page	226
	E-mail Templates	226
	E-mail Templates Overview	227
	Viewing E-mail Templates	228
	Modifying an E-mail Template	228
Chapter 8	Service Central	229
	Service Central Overview	229
	Incidents	232
	Incidents Overview	232
	Assigning an Owner to an Incident	234
	Flagging an Incident to a User	235
	Checking Incident Status Updates	236
	Exporting a Juniper Message Bundle (JMB) to an HTML file	237
	Deleting an Incident	239
	Submitting an Incident to Juniper Support Systems	239
	Viewing Incident Details	244
	Viewing Knowledge Base Articles Associated with an Incident	246
	Uploading an Attachment to an Incident	247
	Updating an End-Customer Case	249
	Uploading Core Files to JSS for an Incident	250
	Technical and End Customer Support Cases	251
	Technical and End Customer Support Cases Overview	251
	Viewing a Case in Case Manager	254
	Uploading an Attachment to a Case	255
	Device Analysis	257
	Exporting BIOS Validation Results	257
	Deleting BIOS Validation Results	258
	Information	259
	Messages Overview	259
	Assigning Ownership to Messages	260
	Flagging a Message to Users	261
	Deleting a Message	261
	Assigning a Message to an End Customer	262
	Device Snapshots Overview	264
	Exporting Device Snapshots to HTML	265
	Generating an On-Demand Device Snapshot	266

	Deleting Device Snapshots	268
	Viewing Details of a Device Snapshot	268
	JMB Errors	270
	JMBs with Errors	270
	Downloading JMBs with Errors	270
	Deleting JMBs with Errors	271
	Notifications	272
	Notification Policies Overview	272
	Creating and Editing a Notification Policy	274
	Enabling or Disabling a Notification Policy	281
	Deleting a Notification Policy	281
Part 3	Junos Space Service Insight	
Chapter 9	Introduction to Service Insight	285
	Service Insight Overview	285
	Service Insight Overview	285
	Service Insight Dashboard	286
	Dashboard Gadgets	287
	Service Insight Domain Overview	289
	Assigning a Service Insight Object to Another Domain	290
Chapter 10	User Roles	291
	Junos Space Service Insight User Roles	291
Chapter 11	Insight Central	293
	Insight Central Overview	293
	Insight Central Overview	293
	Insight Central Overview	293
	Exposure Analyzer	294
	Exposure Analyzer	294
	Exposure Analyzer Overview	294
	Generating EOL Reports	296
	Generating PBN Reports	297
	Showing Matching PBNs	300
	Managing EOL Reports	300
	Managing EOL Reports	300
	EOL Reports Overview	300
	Exporting EOL Reports	302
	Deleting EOL Reports	303
	Regenerating EOL Reports	304
	Managing PBN Reports	305
	PBN Reports Overview	305
	Exporting PBN Reports	306
	Deleting PBN Reports	306
	Regenerating PBN Reports	307

	Managing PBNs	309
	Managing PBNs	309
	Targeted PBNs Overview	309
	Scanning PBNs for Impact on Devices	311
	Flagging PBNs to Users	311
	Assigning an Owner to a PBN	312
	Deleting PBNs	312
	E-Mailing PBNs	313
	Managing Notifications	313
	Managing Notifications	313
	Notifications Overview	314
	Creating and Copying a Notification	315
	Editing the Filters and Actions of a Notification	317
	Enabling and Disabling Notifications	317
	Deleting Notifications	318
Chapter 12	JSS Messages Reference	319
	LIC-1001	319
	LIC-1098	319
	LIC-1099	319
	LIC-2000	320
	LIC-2099	320
	LIC-3000	320
	LIC-4000	320
	LIC-4001	321
	LIC-4002	321
	LIC-4003	321
	LIC-4004	321
	LIC-4005	321
	LIC-4006	322
	LIC-4007	322
	LIC-4008	322
	LIC-4009	322
	LIC-4010	322
	LIC-4011	323
	PAR-3000	323
	PAR-3001	323
	PAR-3002	323
	PAR-3003	323
	PAR-3004	324
	PAR-3005	324
	PAR-3006	324
	PAR-3007	324
	PVS-1000	324
	PVS-1001	325
	PVS-1002	325
	PVS-1006	325
	PVS-1007	325
	PVS-1008	325

PVS-1009	326
PVS-1010	326
PVS-1011	326
PVS-1100	326
PVS-1200	326
PVS-1201	326
PVS-1202	327
PVS-1203	327
PVS-1204	327
PVS-1205	327
PVS-1207	327
PVS-1210	328
PVS-1213	328
PVS-1214	328
PVS-1215	328
PVS-1216	328
PVS-1223	329
PVS-1226	329
PVS-1227	329
PVS-1230	329
PVS-1231	329
PVS-1232	330
PVS-8000	330
PVS-8001	330
PVS-8002	330
PVS-8006	330
PVS-9000	330
PVS-9999	331
SEC-1000	331
SEV-0001	331
SEV-0002	331
SEV-0003	331
VLD-1000	331
VLD-2000	332

Part 3

Index

Index	335
-------------	-----

List of Figures

Chapter 1	Service Automation Overview	21
	Figure 1: Service Automation Solution	23
Part 1	AI-Scripts	
Chapter 2	AI-Scripts Overview	27
	Figure 2: Attachment Section of a JMB	34
	Figure 3: Log Section of a JMB	34
Part 2	Junos Space Service Now	
Chapter 4	Service Now Overview	47
	Figure 4: Service Now Operating in Direct Mode	60
	Figure 5: Service Now Operating in Partner Proxy and End Customer Modes	61
	Figure 6: Platform with Most Incidents Gadget	65
	Figure 7: Devices with Most Incidents Gadget	66
Chapter 7	Administration	91
	Figure 8: Organizations Page	94
	Figure 9: Add Organization Dialog Box	96
	Figure 10: Add Member Dialog Box	99
	Figure 11: Test Connection Dialog Box	102
	Figure 12: Messages Assigned to Connected Member Page	103
	Figure 13: Create Device Group Page	106
	Figure 14: Select Devices to Add to Service Now and Click Submit Page	114
	Figure 15: Install Event Profile Page	115
	Figure 16: Uninstall Event Profiles Dialog Box	118
	Figure 17: On-demand Incident Dialog Box	122
	Figure 18: Create On-demand Incident Status Dialog Box	124
	Figure 19: Configure File Collections Dialog Box	126
	Figure 20: Request RMA page	128
	Figure 21: Configure Maintenance Mode Dialog Box	131
	Figure 22: Modify Auto Submit Policy Page	134
	Figure 23: Service Now Partner Communicating with a Service Now End Customer and JSS Using SSL Certificate	136
	Figure 24: BIOS Validation Legal Notice on Service Now Partner	142
	Figure 25: BIOS Validation Legal Notice on Service Now End Customer	143
	Figure 26: Configure BIOS Validation Dialog Box	146
	Figure 27: Product Health Data Devices Page	148
	Figure 28: View All Product Health Data Files Page	150
	Figure 29: View All Devices of this PHDC Page	152

Figure 30: Product Health Data Collection Page	153
Figure 31: Create PHDC Page	156
Figure 32: Configure Product Health Data Collection	156
Figure 33: Configure Product Health Data Collection Dialog Box	158
Figure 34: Modify Product Health Data Collection Page	161
Figure 35: Modify Product Health Data Collection Parameters	162
Figure 36: Retry on Failed Devices Page	164
Figure 37: Disable Collection on Devices Page	165
Figure 38: Enable Collection on Devices Page	166
Figure 39: Abort Product Health Data Collection Dialog Box	168
Figure 40: PHDC Information of Devices Exported to Excel	169
Figure 41: PHD Files Information Exported to Excel	169
Figure 42: View all Devices of this PHDC	170
Figure 43: View All Product Health Data Files Page	172
Figure 44: View All Devices of this PHDC Page	172
Figure 45: View All Product Health Data Files Page	174
Figure 46: View All Devices of this PHDC Page	174
Figure 47: View all Product Health Data Files Page	176
Figure 48: View Event Profiles Page	178
Figure 49: Install Event Profile Page	179
Figure 50: Uninstall Event Profiles Dialog Box	181
Figure 51: Install Event Profile Page	183
Figure 52: Uninstall Event Profiles Dialog Box	185
Figure 53: Add Event Profile Page	186
Figure 54: Potential Exposure to Known Issues Page	188
Figure 55: View Event Profiles Page	192
Figure 56: Export All Data Dialog Box	193
Figure 57: Export All Data Dialog Box	194
Figure 58: Push to Devices Dialog Box	196
Figure 59: Potential Exposure to Known Issues Page	197
Figure 60: View Event Profiles Page	199
Figure 61: Add Script Bundle Dialog Box	200
Figure 62: Global Settings Page	202
Figure 63: SNMP Trap Attribute Page	207
Figure 64: Core File Upload Configuration Page	209
Figure 65: Auto Submit Policy Page	211
Figure 66: Auto Submit Policy Creation Page	212
Figure 67: Choose Events to Include in Auto Submit Policy Page	213
Figure 68: Change Auto Submit Policy Status Page	217
Figure 69: Change Auto Submit Policy Dampening Status Page	219
Figure 70: Associate Address Group to Devices Page	222
Figure 71: Associate Devices to Address Group Page	224
Figure 72: Associate Devices to Address Group Page	225
Figure 73: E-mail Templates Page	227
Chapter 8 Service Central	229
Figure 74: Service Central Gadgets	230
Figure 75: Export JMB to HTML Dialog Box	238
Figure 76: Submit Case Options Page	241

	Figure 77: Incident Detail Page	246
	Figure 78: Upload Attachment Dialog Box	248
	Figure 79: End-Customer Cases Dialog Box	249
	Figure 80: View Tech Support Cases	251
	Figure 81: View End Customer Cases Page	253
	Figure 82: Upload Attachment Dialog Box	256
	Figure 83: Choose Connected Members Dialog Box	263
	Figure 84: On-demand Incident Dialog Box	266
	Figure 85: Juniper Message Bundle	269
	Figure 86: View JMB Dialog Box	269
	Figure 87: Download JMB Errors Dialog Box	271
	Figure 88: Create Notifications Page	274
Part 3	Junos Space Service Insight	
Chapter 11	Insight Central	293
	Figure 89: Insight Central Landing Page	294
	Figure 90: Exposure Analyzer Page	295
	Figure 91: Generate PBN Report Dialog Box	298
	Figure 92: EOL Reports Page View	301
	Figure 93: Regenerate EOL Report Dialog Box	304
	Figure 94: PBN Reports page	305
	Figure 95: Regenerate PBN Report Dialog Box	308

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xviii
Part 1	AI-Scripts	
Chapter 2	AI-Scripts Overview	27
	Table 2: Elements in the Manifest Section of a JMB	29
Part 2	Junos Space Service Now	
Chapter 4	Service Now Overview	47
	Table 3: Service Now Objects and Their Default Domains	51
	Table 4: Features and Tasks Enabled for Service Now Modes	61
	Table 5: Service Now Workspaces	64
	Table 6: Filter-enabled Tables and Columns	67
	Table 7: Predefined Roles for the Service Now Application	70
Chapter 6	Trouble Ticket APIs Supported by Service Now	75
	Table 8: Trouble Ticket APIs Supported by Service Now	83
	Table 9: OSS/J Client Error Scenarios	84
	Table 10: Supported Trouble Ticket Attributes	87
Chapter 7	Administration	91
	Table 11: Organization Column Descriptions	94
	Table 12: Description of Fields on the Add Organization Page	96
	Table 13: Service Now Devices Field Descriptions	109
	Table 14: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs	123
	Table 15: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs	129
	Table 16: BIOS Validations Field Descriptions	143
	Table 17: Fields on the Product Health Data Devices Page	148
	Table 18: Fields on the View All Product Health Data Files Page	150
	Table 19: Fields on the Product Health Data Collection Page	154
	Table 20: Add Event Profile Page Field Descriptions	186
	Table 21: Global Settings Parameters	203
	Table 22: Icons That Represent the Event Types and Their Descriptions	213
	Table 23: Auto Submit Policy Icons	218
Chapter 8	Service Central	229
	Table 24: Fields on the Incidents Page	233
	Table 25: Fields on the View Tech Support Cases Page	252

	Table 26: Fields on the View End Customer Cases Page	253
	Table 27: BIOS Validation Field Descriptions	257
	Table 28: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs	267
	Table 29: Notification Triggers and Trigger Filters	272
	Table 30: Create Notification Policy Page Field Descriptions	275
Part 3	Junos Space Service Insight	
Chapter 9	Introduction to Service Insight	285
	Table 31: Service Insight Workspaces	287
	Table 32: Service Insight Objects and Their Default Domains	290
Chapter 10	User Roles	291
	Table 33: Predefined Roles for the Service Insight Application	291
Chapter 11	Insight Central	293
	Table 34: Exposure Analyzer Page Icon Descriptions	295
	Table 35: Device Details from the Exposure Analyzer Page	296
	Table 36: EOL Reports Page and EOL Report Detail Dialog Box Fields Description	301
	Table 37: PBN Reports Page and PBN Report Detail Dialog Box Fields Description	305
	Table 38: Manage PBNs Page Fields Description	310
	Table 39: Manage Notifications Page Fields Description	314
	Table 40: Manage Notifications Page Field Description	316

About the Documentation

- Documentation and Release Notes on page xvii
- Documentation Conventions on page xvii
- Documentation Feedback on page xviii
- Requesting Technical Support on page xviii

Documentation and Release Notes

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







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

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

Documentation Conventions

Table 1 on page xviii 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.

- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Service Automation Overview

- [Service Automation Overview on page 21](#)

Service Automation Overview

Juniper Networks Service Automation is an end-to-end solution designed to streamline operations and enable proactive network management of devices running Junos OS. With Service Automation, a network operator can perform the following functions:

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

The Service Automation solution is provided to all customers with Juniper Care and Juniper Care Plus service contracts. Juniper Networks partners can take advantage of Service Automation capabilities through the Operate Services program. For information about the Operate Services program, see [Operate Services Program](#).

Service Automation comprises the following components:

- Advanced Insight-Scripts (AI-Scripts):

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

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

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

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

You can use Service Now to generate a JMB without using AI-Scripts; for example, when you want to check the health of the device well before receiving an iJMB. This JMB is known as an off-box on-demand iJMB. Service Now can also generate off-box on-demand eJMBs and off-box on-demand Return Materials Authorization (RMA) JMBs. Service Now uses the **directive.rc** file to generate the off-box JMBs. The **directive.rc** file in Service Now contains the required commands to generate the JMBs.

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

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

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

- Juniper Support System (JSS):

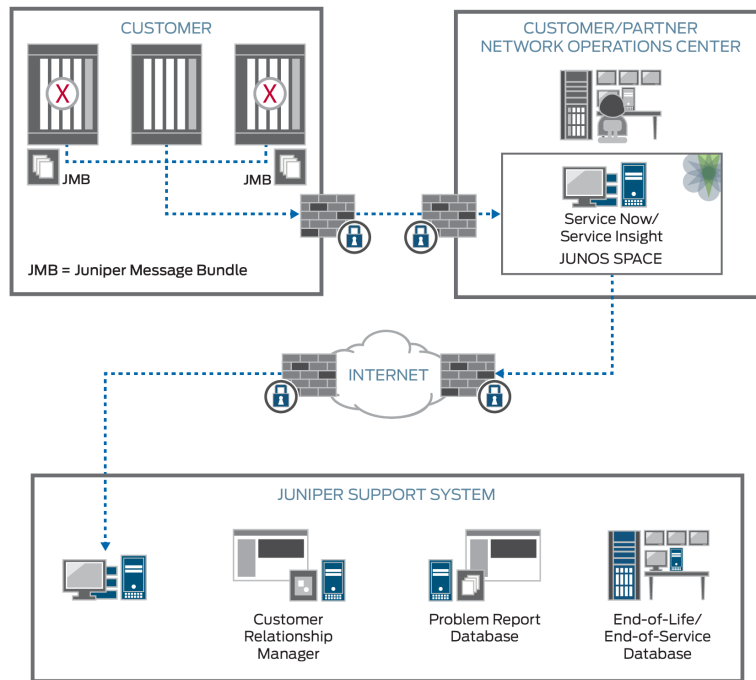
JSS comprises knowledge repositories, such as the EOL or EOS database, the Juniper Customer Relationship Manager (CRM), Juniper Contracts systems, and bugs database.

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

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

[Figure 1 on page 23](#) represents the Service Automation solution.

Figure 1: Service Automation Solution



- Related Documentation**
- [AI-Scripts Overview on page 27](#)
 - [Service Now Overview on page 48](#)
 - [Service Insight Overview on page 285](#)

PART 1

AI-Scripts

- [AI-Scripts Overview on page 27](#)
- [Installing AI-Scripts on page 37](#)

CHAPTER 2

AI-Scripts Overview

- [AI-Scripts Overview 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 Junos Space Service Now” on page 200](#).

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 data about the event, package the data in a structured format called a Juniper Message Bundle (JMB), and store the JMB at a defined location on the device from where Service Now accesses the data for resolution.

This section contains the following topics:

- [Working Modes of AI-Scripts on page 27](#)
- [Events Detected by AI-Scripts on page 28](#)
- [Types of JMBs on page 28](#)
- [JMB Contents on page 29](#)
- [Logs on page 34](#)

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 the 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 the data 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 event 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 request on the 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 as ASIC issues

For a complete list of events detected by AI-Scripts, refer to the latest version of *AI-Scripts Release Notes* at [Service Automation Index Page](#).

Types of JMBs

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

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

An eJMB contains manifest, attachment, and log sections.

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

An iJMB contains manifest, trend data, and attachment sections.

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

When a component fails, the relevant AI-Script in the AI-Scripts bundle is triggered to collect the required data for compiling the RMA JMB and reporting the event.

- On-demand JMBs—On-demand JMBs are generated when a user requests for a JMB to be generated on the device. On-demand JMBs can be of the following types:

On-demand JMBs can be of the following types:

- On-demand JMBs generated by AI-Scripts: AI-Scripts generate on-demand JMBs by using the `/var/db/scripts/on-demand.slax` script present in the AI-Scripts bundle. AI-Scripts can only generate on-demand eJMBs.
- On-demand JMBs generated by Service Now: Service Now generates on-demand JMBs by using the `directive.rc` file packaged with Service Now. The `directive.rc` file contains the commands to generate JMBs.

Service Now can generate the following types of JMBs:

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

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. Elements displayed in the manifest section depend on the type of the JMB.

[Table 2 on page 29](#) lists the elements present in a JMB manifest.

Table 2: Elements in the Manifest Section of a JMB

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

Table 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.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • Event: The JMB is generated in response to an event that occurred on the device. (This is a reactive measure.) • Intelligence: The JMB is generated and collected periodically to monitor the vital functions of the device. (This is a proactive measure.) • On-demand: The JMB is generated in response to a request from a user. • Event-RMA: The JMB is generated in response to an Return Material Authorization (RMA) event on the device. This is a reactive measure. • Health-check: The JMB is generated and collected periodically to check the integrity of the BIOS or for any errors related to the AI-Scripts installed on the device. This is a proactive measure.
Time Occurred	Specifies the time at which the event occurred
Event Type Group	<p>Classifies the events that occurred on the device under the following categories:</p> <ul style="list-style-type: none"> • Hardware failure • Software failure • Resource exhaustion <p>This field is not applicable for an iJMB.</p>
Event Type	<p>Specifies the type of event that occurred on the device; for example, MAC error or Process error</p> <p>This field is not applicable for an iJMB.</p>
Problem Synopsis	<p>Specifies a summary of the event; this field is used to populate the Problem Synopsis field in the CRM.</p> <p>This field can be appended with your text while submitting the incident for resolution to JSS or a Service Now partner.</p> <p>This field is not applicable for an iJMB.</p>

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

Element	Description
Problem Description	<p>Describes the event; this field is used to populate the Problem Description field in the CRM.</p> <p>This field can be appended with your text while submitting the incident for resolution.</p> <p>This field is not applicable for an iJMB.</p>
Problem Severity	<p>Specifies JTAC's assessment of the impact that the event has on the customer's network</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low <p>This field is not applicable for an iJMB.</p>
Problem Priority	<p>Specifies the customer's perception of the impact that the event has on the network; this field is used to populate the Problem Priority field in the CRM system.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low <p>This field is not applicable for an iJMB.</p>
KBURL	<p>Specifies the link to the knowledge base (KB) article related to the event</p> <p>This field is not applicable for an iJMB.</p>
AI-Script Version	Specifies the version of the AI-Scripts that generated the JMB
Associated Core File	<p>Specifies the core files included in the JMB</p> <p>This field is not applicable for an iJMB.</p>
Router Information	
Product Name	Specifies the name of the product; this field is used to populate the Platform field in CRM.
Host Name	Specifies the hostname assigned to the device

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

Element	Description
OS Platform	Specifies the routing OS installed on the device
Routing Engine	
Name	Specifies the name of the Routing Engine
Mastership State	Specifies whether the Routing Engine serves as the primary or the backup Routing Engine of the device
Component	Specifies the components of Junos OS such as rpd and chassisd
Version	Version of Junos OS component executing on the Routing Engine
Builder	User who created the Junos OS build
Build Date	Date and time the Junos OS build was created
Service Now Information	
RSI Collection	Specifies the configuration for collecting Request Support Information (RSI) from the device—whether RSI collection is enabled or disabled and the interval for collecting RSI
BIOS Validation	Specifies whether BIOS validation is enabled or disabled on the device
Log Collection	Specifies whether log collection is enabled or disabled on the device True indicates that log collection is enabled and False indicates that log collection is disabled.
Space Platform Version	Specifies the version of Junos Space Network Management Platform managing the device
Service Insight	Specifies the version of Service Insight installed with Service Now
Service Now	Specifies the version of Service Now managing the device
AI-Scripts Information	

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

Element	Description
RSI Collection	Specifies the configuration for collecting Request Support Information (RSI) from the device—whether RSI collection is enabled or disabled and the interval for collecting RSI
Log Collection Enabled	Specifies whether log collection is enabled or disabled on the device True indicates that log collection is enabled and False indicates that log collection is disabled.
BIOS Validation	Specifies whether BIOS validation is enabled or disabled on the device
PHD Collection	Specifies whether collection of product health data (PHD) is enabled or disabled on the device
PHD Collection Commands File	Specifies the file that contains the commands to collect PHD on the device
JMB Cleanup Interval	Specifies the interval in seconds after which JMBs generated due to PHD collection are deleted

- Trend data: 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 the 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**

From Service Now Release 14.1R3 onwards, the attachments of an off-box on-demand JMB also include information about the last four configuration changes made on the device.

The attachment files are retrieved from the device and stored in the Service Now database. The JMB contains links to view and download attachment files.

Figure 2 on page 34 shows the Attachment section of a JMB.

Figure 2: Attachment Section of a JMB

Juniper Message Bundle (JMB)						
Attachments details			Click here to download all attachments			
Name	Command	File type	Size (Bytes)	View	Download	
bng-fbox1-reg-20150404-093010303_196621_att_ach_shd_xml	show chassis hardware	xml	1526	View	Download	
bng-fbox1-reg-20150404-093010306_196621_att_ach_rsi	request support information	text	793761	View	Download	
bng-fbox1-reg-20150404-093010308_196621_att_ach_AISESI	multiple	text	55659	View	Download	
bng-fbox1-reg-20150404-093010310_196621_att_ach_cfg_xml	show configuration display inheritance	xml	2433	View	Download	
bng-fbox1-reg-20150404-093010312_196621_att_ach_ver_xml	show version	xml	702	View	Download	
bng-fbox1-reg-20150404-093010314_196621_att_ach_statusmsgs	N/A	text	10859	View	Download	

Logs

This section contains a compressed view of the **/var/log** directory of the device. However, if the **/var/tmp** directory has less than 20% of the required free space, the contents are collected in an attachment.

The log files are retrieved from the device and stored in the Service Now database. The JMB contains the links to view and download the log files.

Figure 3 on page 34 shows the log section of a JMB.

Figure 3: Log Section of a JMB

Juniper Message Bundle (JMB)						
Manifest						
Attachments						
Logs file details			Click here to download all logs			
Logs	Name	File type	Size (Bytes)	Created	View	Download
	snk-1400-sn1-20150617-002531854_262184_attach_logs_lgz	zip	23087321	2015-06-17 00:25:32	-	Download

- Related Documentation**
- [Adding a Script Bundle to Junos Space Service Now on page 200](#)
 - [Deleting a Script Bundle from Junos Space Service Now on page 201](#)

CHAPTER 3

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 Junos Space Service Now” on page 200](#).
- 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 39](#).

AI-Scripts System Requirements

AI-Scripts can be installed and run on devices running Junos OS Release 11.4 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 37](#)
- [AI-Scripts Install Package Versioning on page 38](#)
- [AI-Scripts Install Locations on Devices on page 39](#)
- [Automatically Installing AI-Scripts Bundles on page 39](#)
- [Manually Installing AI-Scripts on Devices on page 39](#)

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 Junos Space Service Now” on page 200](#).

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.



NOTE: We recommend that you install AI-Scripts on devices during a maintenance window.

To install AI-Scripts manually for Release 4.XRX or earlier:

1. Copy the AI-Scripts install package (example: `jais-4.0R1.0-signed.tgz`) to the Junos OS device using SCP or FTP.
2. Install the AI-Scripts bundle install package in CLI mode by using one of the following commands:
 - **request system scripts add <pathname>**, where `<pathname>` is the path to the AI-Scripts bundle copied on the device.

- **request system software add** *<package-name>* *<node>*, where *<node>* is the Routing Engine—re0 or re1 and *<package-name>* is the name of the AI-Scripts bundle copied on the device.



NOTE:

- The **request system software add** *<pathname>* *<node>* command when executed on a master Routing Engine installs AI-Scripts on all backup Routing Engines of a device.
- We recommend that the AI-Scripts installation package be placed in the `/var/tmp/` directory as some platforms require the package to be stored in the `/var/tmp/` directory.
- 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.

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

3. Verify that AI-Scripts is installed on all Routing Engines of the device by using the **show version** command.
4. 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/



NOTE: For QFabric devices, use the following command:

set fabric administration ais enable

5. Commit the static AI-Scripts configuration.

To manually install AI-Scripts Release 5.0R1 or later on a device:



BEST PRACTICE: We recommend you to use Service Now to install AI-Scripts Release 5.0R1.0 and later. For information about installing AI-Scripts Release 5.0R1.0 and later on a device by using Service Now, see [“Installing an Event Profile on a Device by Using Service Now” on page 114](#).



NOTE: AI-Scripts Release 5.0R1 or later cannot be installed on QFabric devices.

1. Copy the AI-Scripts install package (example: jais-5.0R1.0-signed.tgz) to the Junos OS device using SCP or FTP.
2. Install the AI-Scripts bundle install package in CLI mode by using one of the following commands:
 - **request system scripts add <pathname>**, where <pathname> is the path to the AI-Scripts bundle copied on the device.
 - **request system software add <pathname> <node>**, where <node> is the Routing Engine—re0 or re1 and <package-name> is the name of the AI-Scripts bundle copied on the device.



NOTE:

- The **request system software add <pathname> <node>** command when executed on a master Routing Engine installs AI-Scripts on all backup Routing Engines of a device.
- We recommend that the AI-Scripts installation package be placed in the /var/tmp/ directory as some platforms require the package to be stored in the /var/tmp/ directory.
- 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.

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

3. Verify that AI-Scripts is installed on all Routing Engines of the device by using the **show version** command.
4. For AI-Scripts Release 5.0R1 and later, enter the configuration mode on the device and add the static AI-Scripts configuration as follows:

```
set groups juniper-ais system scripts op file ais_change_perm.slax
set groups juniper-ais system scripts op file ais_core_perm.slax
set groups juniper-ais system scripts op file on-demand.slax
set groups juniper-ais system scripts op file remove-jais.slax
```

```

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

```

5. Commit the static AI-Scripts configuration.



BEST PRACTICE: We recommend that you commit the AI-Scripts configuration during a maintenance window.

On a multichassis system, use the `commit synchronize` command so that the AI-Scripts configuration is committed on all Routing Engines.

6. Do one of the following to activate the event profile

- If using the **AISevent_info_default.xml** file to define the event profile, edit the **AISevent_info_default.xml** file to include the events that you want to monitor on the device.

The **AISevent_info_default.xml** file is present at the **/var/db/scripts/commit** location and includes all the event definitions that are available for a release. The default event profile automatically excludes events that are not valid for a device.

Use the **op ais-param-set event-file default** command to activate the event profile.



BEST PRACTICE: On a multichassis system, execute the command on the master Routing Engine.

- If using the **AISBundle_info.xml** file to define event profile, verify that the **AISBundle_info.xml** file is present in the **//var/db/scripts/commit/** location.

The file contains the definitions for the events to be monitored on the system and is stored on the device by Service Now while installing Service Now.

Use the **op ais-param-set event-file /var/db/scripts/commit/AISBundle_info.xml** command to activate the event profile.

The event profile is installed and configured on the device.

**Related
Documentation**

- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Adding a Script Bundle to Junos Space Service Now on page 200](#)

PART 2

Junos Space Service Now

- [Service Now Overview on page 47](#)
- [Using the Service Now Getting Started Assistant on page 73](#)
- [Trouble Ticket APIs Supported by Service Now on page 75](#)
- [Administration on page 91](#)
- [Service Central on page 229](#)

CHAPTER 4

Service Now Overview

- [Service Now Overview on page 48](#)
- [Installing, Upgrading, and Uninstalling Junos Space Service Now and Junos Space Service Insight Applications on page 53](#)
- [Service Now MIBs on page 57](#)
- [Service Now Modes on page 58](#)
- [Service Now Dashboard and Workspaces Overview on page 62](#)
- [Service Now Inventory Pages on page 66](#)
- [User Roles on page 69](#)

Service Now Overview

- [Junos Space Service Now Overview on page 48](#)
- [Service Now Domain on page 50](#)

Junos Space Service Now Overview

Junos Space Service Now is an application that runs on the Junos Space Network Management Platform to automate fault management and accelerate issue resolution. This application 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 standalone 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 about Service Now modes, see *Service Now Modes*.

Service Now receives information about events, such as a process crash, an ASIC error, or a fan failure, when they occur on a device from AI-Scripts installed on the device. AI-Scripts detect an event on the device on which they are installed and automatically collect diagnostic data for the event and package the data into an XML file called *Juniper Message Bundle* (JMB).

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

- **Reactive mode:** In reactive mode, the AI-Scripts collect data from the 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.

An eJMB usually includes the device identity, the problem event, log files, and core files. This information is securely transferred to the Junos Space Platform. Service Now creates an incident in response to the event and the received JMB. Service Now then notifies users about the new incident by sending an e-mail or an SNMP trap.
- **Proactive mode:** In proactive mode, the AI-Scripts periodically collect data on vital system functions and store the data 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 event 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 the device by using Service Now, Service Now generates an on-demand incident JMB by executing preconfigured CLIs on the device.

Service Now categorizes the JMBs that do not comply with the defined standard data structure or that contain unexpected data elements as error JMBs. Service Now displays the error JMBs on the JMB Errors page. From the JMB Errors page, you can view and download the error JMBs.

In response to a JMB collected from a device, Service Now creates an incident and notifies users about the incident by sending an e-mail or an SNMP trap. You can submit the incident to Juniper Support Systems (JSS), after reviewing the information provided in the JMB, to create a Juniper Networks Technical Assistance Center (JTAC) case. You can also configure Service Now to submit an incident automatically to JSS as soon as the incident is created. Service Now provides an option to filter the device configuration information from a JMB before you share the information with JSS or a Service Now partner (if Service Now is operating in end customer mode).

JSS sends updates to Service Now for you to track the status of the case.

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.
- Keep users informed about changes made to the incident.
- Set up notification policies for users who need to be kept informed about 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 or CSV format and store the data on the local file system.

To submit incidents, share JMBs, and open support cases with JSS, you must first configure 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. To add multiple organizations and devices to Service Now, you need to obtain a technical support contract with the level of service that you require. 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 with JSS or open technical support cases with JTAC.

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.

For Service Now to monitor and detect events on devices, you must discover the devices by using the Junos Space Network Management Platform, add the devices to Service Now, and then install AI-Scripts on the devices. You can categorize the devices into device groups to manage the devices as a single entity. For example, you can install or remove AI-Scripts simultaneously on all devices in a device group. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses.

Service Now also sends SNMP traps if notification policies are configured to send traps when events occur on devices. From Service Now Release 14.1 and Service Insight Release 14.1, Service Now and Service Insight use proxy server configured on the Junos Space Platform to facilitate all communication over the Internet.

The Service Now dashboard displays the gadgets and workspaces that the user can use to perform various tasks. For more information about the Service Now dashboard, see [“Service Now Dashboard Overview” on page 63](#).

From the Release 14.1 of Junos Space Platform, Service Now, and Service Insight, Service Now and Service Insight are available as hot-pluggable applications. This makes it possible for you to install, upgrade, and uninstall Service Now and Service Insight applications independently of the Junos Space Platform. See the *installing, Upgrading, and Uninstalling Junos Space Service Now* section of the *Service Automation Quick Start Guide* for information about installing, upgrading, and uninstalling Service Now and Service Insight.

To install, upgrade, and uninstall Service Now from a Junos Space server, you need Junos Space administrator privileges. You can install, remove, or upgrade Service Now even while Junos Space and Junos Space applications are still running. Refer to [“Junos Space Service Now User Roles” on page 69](#) for information about user roles and tasks that can be performed for a user role.

Related Documentation

- [Service Central Overview on page 229](#)
- [Administration Overview on page 91](#)
- [Service Now Domain on page 50](#)
- [Insight Central Overview on page 293](#)

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 52](#).

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 51](#) 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

Table 3: Service Now Objects and Their Default Domains (*continued*)

Service Now Objects	Default Domain	
	Fresh Installation	Migration
<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 229](#)
 - [Administration Overview on page 91](#)
 - [Domains Overview](#)

Installing, Upgrading, and Uninstalling Junos Space Service Now and Junos Space Service Insight Applications

From Release 14.1 of Junos Space Network Management Platform, Junos Space Service Now, and Junos Space Service Insight, Junos Space Service Now and Junos Space Service Insight are available as hot-pluggable applications. This makes it possible for you to install, upgrade, and uninstall Service Now and Service Insight independently of the Junos Space Platform.



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

This topic contains the following sections:

- [Uploading a Service Now Image File to Junos Space server on page 53](#)
- [Installing Junos Space Service Now and Junos Space Service Insight on page 54](#)
- [Upgrading Junos Space Service Now and Junos Space Service Insight on page 56](#)
- [Uninstalling Junos Space Service Now and Junos Space Service Insight on page 57](#)

Uploading a Service Now Image File to Junos Space server

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

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

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

The Applications page appears.

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



The Add Application page appears.

5. On the Add Application page, perform one of the following tasks:
 - Upload the Service Now image file by using HTTP.
 - a. Click **Upload via HTTP**.

The Upload Software via HTTP dialog box appears.

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



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

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

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

The Upload Software via SCP dialog box appears.
 - b. Enter the following details for the image file to be uploaded by using SCP:
 - Username: Enter your username for the local file system.
 - Password: Enter your password for the local file system.
 - Confirm Password: Retype your password.
 - Machine IP: Enter the host IP address of the local file system.
 - Software File Path: Specify the file path to access the Service Now image file on the local file system.
 - c. Click **Upload**.

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

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

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

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

The Applications page appears.

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

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

Installing Junos Space Service Now and Junos Space Service Insight

Before you install Junos Space Service Now and Junos Space Service Insight:

- Ensure that the versions of Service Now and Service Insight that you want to install are compatible with the version of the Junos Space Network Management Platform installed on the Junos Space Server. For information about the compatibility of the

Service Now and Service Insight with Junos Space Platform, refer to <http://kb.juniper.net/InfoCenter/index?page=content&id=KB27572>.

If the installed Junos Space Platform version is earlier than the compatible version, upgrade the Junos Space Platform to a compatible version first and then upgrade the Service Now and Service Insight applications. For information about upgrading the Junos Space Platform, refer to *How Do I Upgrade Junos Space?*

- Upload the Service Now image file to a Junos Space server. See “[Uploading a Service Now Image File to Junos Space server](#)” on page 53 for information about uploading an image file to the Junos Space server.



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

To install Service Now and Service Insight applications:

1. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).

2. From the navigation tree, select **Administration > Applications**.

The Applications page appears.

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



The Add Application page appears.

4. On the Add Application page, perform one of the following tasks:
 - If Service Now Release 15.1 is listed, select **Service Now Release 15.1** and then click **Install**.
 - If Service Now Release 15.1 is not listed, upload the Service Now Release 15.1 image file to the Junos Space server.

To upload the Service Now Release 15.1 image file to the Junos Space server, see “[Uploading a Service Now Image File to Junos Space server](#)” on page 53.

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

5. In the Application Management Job Information dialog box, click the *Job ID* link. The Job Management page is displayed. This page displays the progress of the upload job.
6. After the installation job is complete, log out of Junos Space and log in to access Service Now or Service Insight.

Upgrading Junos Space Service Now and Junos Space Service Insight

You can upgrade Junos Space Service Now and Junos Space Service Insight to up to two releases later than the currently installed release. For example, you can upgrade to Service Now Release 15.1 and Service Insight Release 15.1 from the following releases:

- Service Now Release 14.1 and Service Insight Release 14.1
- Service Now Release 13.3 and Service Insight Release 13.3

Service Insight is bundled with the Service Now image file and is upgraded along with Service Now.



CAUTION: Do not uninstall the installed versions of Service Now and Service Insight for upgrading to later versions. Uninstalling the applications deletes all Service Now and Service Insight data from the Junos Space server.

Before you upgrade Junos Space Service Now and Junos Space Service Insight:

- Ensure that versions of Service Now and Service Insight to which you want to upgrade are compatible with the Junos Space Platform version installed on the Junos Space server. For information about compatibility of Service Now and Service Insight with Junos Space Platform, refer to <http://kb.juniper.net/InfoCenter/index?page=content&id=KB27572>.

If the installed Junos Space Platform version is earlier than the compatible version, upgrade the Junos Space Platform to a compatible release first and then upgrade the Service Now and Service Insight applications. For information about upgrading the Junos Space Platform, refer to *How Do I Upgrade Junos Space?*

- Upload the Service Now image file to the Junos Space server. See “[Uploading a Service Now Image File to Junos Space server](#)” on page 53 for information about uploading a Service Now image file to a Junos Space server.

To upgrade Junos Space Service Now and Junos Space Service Insight applications:

1. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).
2. From the navigation tree, select **Administration > Applications**.
The Applications page appears.
3. On the Applications page, click **Service Now** and select **Actions > Upgrade Application**. Alternatively, right-click **Service Now** and select **Upgrade Application**.
The Upgrade Application page appears displaying all the previously uploaded versions of Service Now.
4. On the Upgrade Application page, perform one of the following tasks:
 - If the Service Now release to which you want to upgrade is listed, select the **Service Now release** to which you want to upgrade and click **Upgrade**.

- If the Service Now release to which you want to upgrade is not listed, upload the Service Now image file to the Junos Space server and then click **Upgrade**.

To upload a Service Now image file to the Junos Space server, see [“Uploading a Service Now Image File to Junos Space server” on page 53](#).

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

5. In the Application Management Job Information dialog box, click the **Job ID** link. The Job Management page is displayed. This page displays the progress of the upload job.
6. After the upgrade job is complete, navigate to **Administration > Applications**.

The Applications page lists the upgraded releases of Service Now and Service Insight.

Uninstalling Junos Space Service Now and Junos Space Service Insight

When you uninstall Junos Space Service Now operating in end customer mode, the corresponding connected member in the Service Now partner is deactivated—that is, the connection status of the connected member appears as **Deactivated** on the Organization Details page of the Service Now partner.

When you uninstall Service Now, Junos Space Service Insight is uninstalled along with Service Now; Service Insight is uninstalled first followed by Service Now.



NOTE: Before uninstalling the Service Now and Service Insight applications, ensure that you remove devices that have AI-Scripts installed on them from Service Now. Otherwise, the uninstallation of Service Now and Service Insight fails.

To uninstall Service Now and Service Insight applications:

1. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).
2. From the navigation tree, select **Administration > Applications**.

The Applications page appears.

3. On the Applications page, click **Service Now** and select **Actions > Uninstall Application**. Alternatively, right-click Service Now and select **Uninstall Application**.

The progress of the uninstallation process is displayed. After the uninstallation is complete, Service Now and Service Insight applications are not listed on the Applications page.

Service Now MIBs

- [Service Now MIBs on page 58](#)

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 274](#).

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 Configuration to Service Now on page 204](#)
- [Junos Space Service Now Overview on page 48](#)
- [Service Now MIBs Downloads](#)

Service Now Modes

- [Junos Space Service Now Modes on page 59](#)

Junos Space Service Now Modes

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

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

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

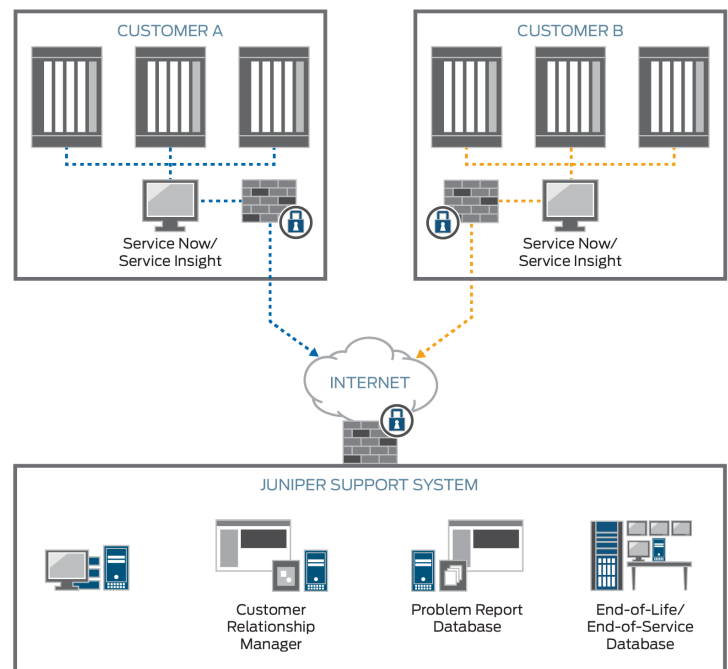
- Demo mode—Service Now operates in Demo mode from the time you install Service Now on Junos Space Network Management Platform until you create an organization and validate the organization by establishing a connection with JSS or a Service Now partner.

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

- Offline mode—You can accept a Direct or Partner Proxy license file and activate the Junos Space Platform and Service Now application without having to connect to JSS. You can perform all Service Now tasks except submit incidents, create autosubmit policies, view exposures, or view cases in Case Manager. If Service Now is already in End Customer mode, you cannot operate it in Offline mode.
- Direct mode—In Direct mode, you can add multiple Service Now organizations and devices in Service Now. Service Now is connected to JSS, which enables you to submit incidents to JSS and JSS to provide support for the incidents that you submit.

Figure 4 on page 60 shows Service Now operating in Direct mode.

Figure 4: Service Now Operating in Direct Mode



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

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

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

You can configure only one organization, but can manage multiple devices in this mode. [Figure 5 on page 61](#) shows Service Now operating in Partner Proxy and End Customer modes.

Figure 5: Service Now Operating in Partner Proxy and End Customer Modes

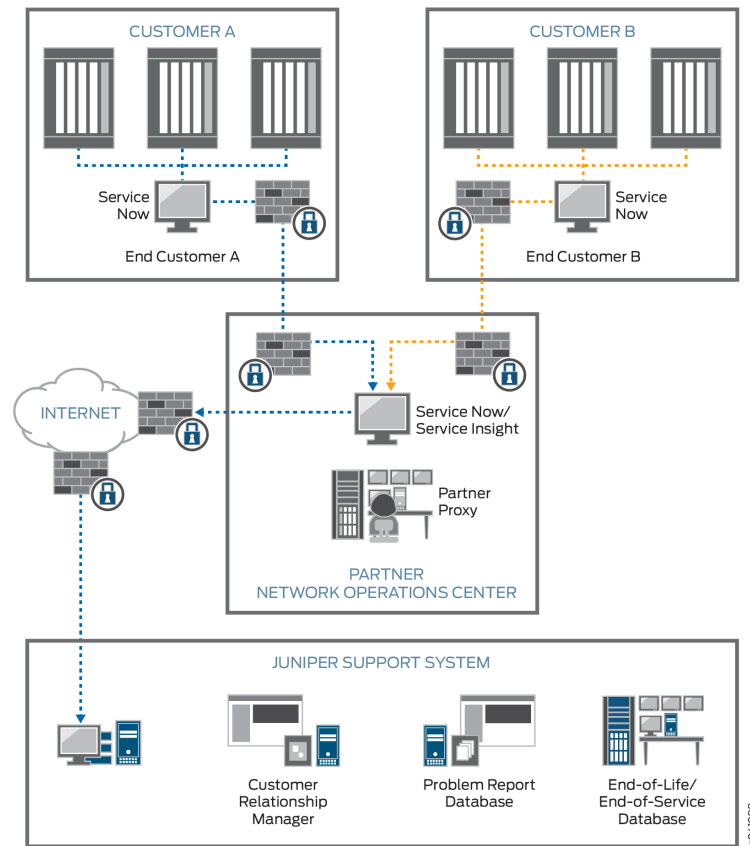


Table 4 on page 61 highlights some of the differences among the various modes of operating Service Now.

Table 4: Features and Tasks Enabled for Service Now Modes

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Number of devices supported	5	Multiple	Multiple	Multiple	Multiple
Number of organizations supported	1	Multiple	Multiple	Multiple	1
Adding connected members	—	—	—	Enabled	—
Updating end-customer cases	—	—	—	Enabled	—

Table 4: Features and Tasks Enabled for Service Now Modes (*continued*)

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Assigning messages to an end - customer	–	–	–	Enabled	–
Viewing messages assigned to an end - customer	–	–	–	Enabled	–
Submitting incidents for creating technical support cases to JSS	Disabled	–	Enabled	Enabled	Disabled (but can submit incidents to the Service Now partner)
Installing or removing AI-Scripts on or from devices	Enabled	Enabled	Enabled	Enabled (only for devices managed directly by the Service Now partner)	Enabled
Validating the BIOS	Disabled	–	Enabled	Enabled	Enabled
Product Health Data Collection	–	–	Enabled	Enabled	–
Other tasks (viewing incidents, configuring notifications, receiving JMBs, managing the inventory, and so on)	Enabled	Enabled	Enabled	Enabled	Enabled

Related Documentation

- [Administration Overview on page 91](#)
- [Service Central Overview on page 229](#)
- [Configuring Global Settings on page 202](#)
- [Adding an Organization to Service Now on page 95](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 98](#)

Service Now Dashboard and Workspaces Overview

- [Service Now Dashboard Overview on page 63](#)

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 63](#)
- [Dashboard Gadgets on page 64](#)

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 *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 64](#) 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 devices from which BIOS data is collected and the time BIOS data was collected. View devices from which product health data is collected and the product health data files collected from the devices. 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. Configure product health data collection on devices. Export inventory information in CSV format. Configure the global settings (SNMP server and core file upload). 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:

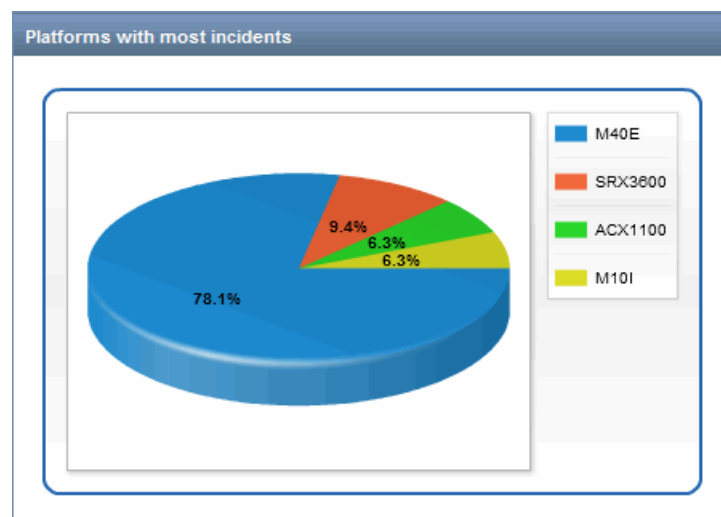
- [Platforms with Most Incidents on page 65](#)
- [Devices with the Most Incidents on page 65](#)
- [Service Now Notices \(Upgrade and Contract Notice\) on page 66](#)

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 6 on page 65](#)), the Incidents page displays only those incidents that are detected on the ACX1100 router.

Figure 6: Platform with Most Incidents Gadget

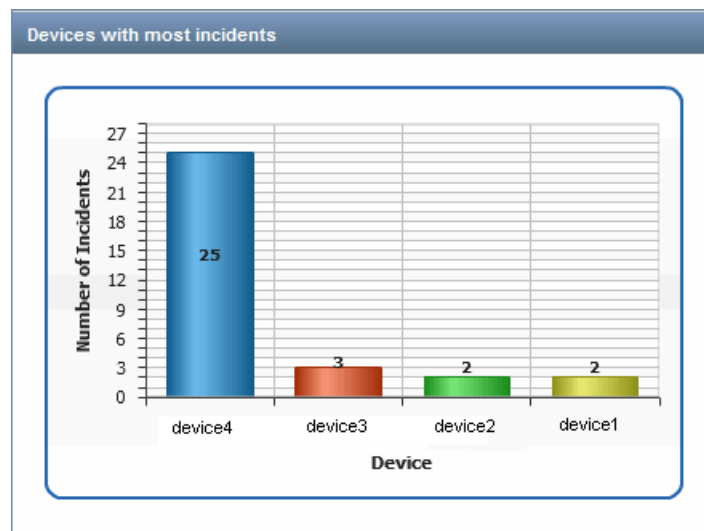


Devices with the Most Incidents

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 7 on page 66](#), 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 device1.

Figure 7: 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 229](#)
 - [Administration Overview on page 91](#)

Service Now Inventory Pages

- [Filtering Inventory Pages on Service Now and Service Insight on page 66](#)

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 67](#) 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
	Product Health Data Collection	All columns except Devices
	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
	BIOS Validations	All columns except: <ul style="list-style-type: none"> • Connected Member (in Partner Proxy mode) • Junos Version
	Product Health Data Devices	All columns except View.
	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 Central Workspace Overview on page 229](#)
 - [Table 31 on page 287](#)

User Roles

- [Junos Space Service Now User Roles on page 69](#)

Junos Space 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. [Table 7 on page 70](#) lists the predefined roles available in Junos Space Service Now.

Table 7: Predefined Roles for the Service Now Application

Role	Workspace	Task Groups and Tasks
Service Now Admin	Administration	<ul style="list-style-type: none"> • Global Settings: Configure an FTP server for uploading core files, manage SNMP traps, and configure Service Now partner certificates on a Service Now end customer • Address Group: Create address groups, associate address groups with devices, modify address groups, delete address groups, and assign address groups to domains • Device Groups: Create device groups, modify device groups, set a device group as the default device group, associate address groups with device groups, assign device groups to domains, and delete device groups from Service Now • Service Now Devices: Add devices to Service Now, export device inventory information, associate devices with autosubmit policies, associate devices with device groups, check FTP server configuration, configure RSI and log file collection on devices, create on-demand incidents, associate devices with address groups, export device information, install event profiles on devices, request Return Materials Authorisation (RMA), uninstall event profile from devices, view exposure of devices to known events, view incidents generated on Service Now, assign the Service Now devices to domains, and delete devices from Service Now • Email Templates: Modify default content of an Email template and restore the modified content of an Email template to its default content • Event Profiles: Add AI-Scripts bundles to Service Now, set an AI-Scripts bundle as the default AI-Scripts bundle in Service Now, delete AI-Script bundles, create event profiles, import event profiles, export event profiles to an XML file, push event profiles to devices, clone event profiles, set an event profile as the default profile, view events included in event profiles, view devices associated with event profiles, assign event profiles to domains, and delete event profiles from Service Now • Auto Submit Policy: Create autosubmit policies, export incident reports, modify autosubmit policies, change the dampening status of autosubmit policies, assign autosubmit policies to a domain, and delete autosubmit policies from Service Now • Organization: Add an organization to Service Now, add end customers to organizations, check the connection status of Service Now with Juniper Support System (JSS) or with a Service Now partner, modify organizations, associate address groups with organizations, delete organizations, update core file upload configuration, view information messages received from JSS, and assign organizations to domains • Product Health Data Collection (PHDC): Configure PHDC, modify PHDC, delete PHDC, enable PHDC on devices, disable PHDC on devices, reschedule PHDC on devices, retry PHDC on failed devices, abort PHDC on devices, delete product health data (PHD) files, download product health data files, export information about product health data and devices
	Service Central	

Table 7: Predefined Roles for the Service Now Application (*continued*)

Role	Workspace	Task Groups and Tasks
		<ul style="list-style-type: none"> • Incidents: Create autosubmit policies, view end-customer cases in Case Manager, update end-customer cases, export JMB to HTML, export incident summaries to Excel, assign an owner to incidents, view end-customer cases created in Service Now, flag incidents to users, submit cases to JSS or a Service Now partner, view KB articles related to an incident, delete incidents, view tech support cases in Case Manager, update tech support cases, upload core files to JSS, Upload attachments to cases, and view JMB associated with an incident • Information: View iJMBs, export iJMBs to HTML, delete iJMBs, assign messages received from JSS to connected members, assign ownership to messages, delete messages, Flag messages to users, and scan devices for impact based on messages received from JSS • View Tech Support Cases: View cases in Case Manager, update cases, and upload text or binary attachments to cases • View End Customer Cases: View end-customer cases in Case Manager and Update end-customer cases • Device Analysis: Delete BIOS validations, export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • JMB Errors: Download error JMBs and delete error JMBs • Notifications: Create notifications, edit notification filters and actions, copy notifications, delete notifications, enable or disable notifications, and assign notifications to domains
Service Now Read Only	Administration	Service Now Devices: Export event profiles, export devices, view exposure of devices to known events, and create on-demand device snapshots, export information about product health data and devices, download product health data files
	Service Central	<ul style="list-style-type: none"> • Incidents: Export a JMB in HTML format, view JMBs, export incident summary to Excel, and view tech support and end-customer cases in Case Manager • JMB Errors: Download error JMBs • Tech Support cases: View tech support cases in Case Manager and update cases • Information: View iJMBs, export iJMBs to HTML and scan devices for impact based on messages received from JSS • Device Analysis: Export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • Notifications: Create notifications • End-customer cases: View end-customer cases in Case Manager

Table 7: Predefined Roles for the Service Now Application (*continued*)

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

To create and manage users, on the Junos Space Network Management Platform GUI, select **Network Management Platform > Role Based Access Control > User Accounts**. The User Accounts page lists the existing users. Use this page to create and assign roles to Service Now and Service Insight users.

For information about creating users, see *Creating Users in Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide* available at

http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html.

**Related
Documentation**

- [Service Central Overview on page 229](#)
- [Administration Overview on page 91](#)
- *Creating Users in Junos Space Network Management Platform*

CHAPTER 5

Using the Service Now Getting Started Assistant

- [Service Now Getting Started Assistant Usage Overview on page 73](#)

Service Now Getting Started Assistant Usage Overview

- [Service Now Getting Started Assistant Usage Overview on page 73](#)

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 Direct mode for Service Now.

The following steps are required:

1. Review Global Settings.
See [“Configuring Global Settings” on page 202](#).
2. Create an Organization.
See [“Adding an Organization to Service Now” on page 95](#).
3. Add Devices to Junos Space.
See the *Discovering Devices* section of the *Junos Space Network Management Platform User Guide*.
4. Create a Device Group.

See [“Creating a Device Group” on page 105](#).

5. Install Scripts using Service Now Devices.

See [“Installing an Event Profile on a Device by Using Service Now” on page 114](#).

The following step is optional:

- Add a New Script Bundle.

See [“Adding a Script Bundle to Junos Space Service Now” on page 200](#).

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*.

**Related
Documentation**

- [Junos Space Service Now Overview on page 48](#)

CHAPTER 6

Trouble Ticket APIs Supported by Service Now

- [Trouble Ticket APIs Overview on page 75](#)
- [Profiles Used by Service Now on page 76](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)

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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Setting up Java Based Web Service Client on page 76](#)

- [Profiles Used by Service Now on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

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.wsdl.troubleticket.v1_2.JVTTroubleTicketSessionWSPort;
import org.ossj.wsdl.troubleticket.v1_2.JVTTroubleTicketSessionWebService;
import org.ossj.xml.common.ArrayOfString;
import org.ossj.xml.troubleticket.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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Accessing a Web Service on page 82](#)
- [Profiles Used by Service Now on page 76](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Profiles Used by Service Now on page 76](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

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**

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Profiles Used by Service Now on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Profiles Used by Service Now on page 76](#)

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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Events Supported by Service Now on page 88](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Profiles Used by Service Now on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

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 86. 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 86](#). 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

- [Junos Space Service Now Overview on page 48](#)
- [Trouble Ticket APIs Overview on page 75](#)
- [Trouble Ticket APIs Supported by Service Now on page 83](#)
- [Trouble Ticket Attributes Supported by Service Now on page 86](#)
- [Setting up Java Based Web Service Client on page 76](#)
- [Profiles Used by Service Now on page 76](#)
- [Accessing a Web Service on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 84](#)

CHAPTER 7

Administration

- [Administration Overview on page 91](#)
- [Organizations on page 92](#)
- [Device Groups on page 104](#)
- [Service Now Devices on page 108](#)
- [BIOS Validation on page 141](#)
- [Product Health Data Collection on page 147](#)
- [Event Profiles and AI-Scripts on page 176](#)
- [Global Settings on page 202](#)
- [Auto Submit Policy on page 210](#)
- [Address Group on page 219](#)
- [E-mail Templates on page 226](#)

Administration Overview

Service Now helps 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 event and informational Juniper Message Bundles (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 Customer Relationship Manager (CRM) systems. After creating an organization, you can test its connectivity with Juniper Support System (JSS) and even run it in test mode. 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 submitting incidents to JSS and configuring BIOS collection are enabled only when Service Now is operating in certain modes. For more information about Service Now modes, see *Service Now Modes*.

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 from devices.
- Associate devices with device groups.
- Add, modify, or delete organizations.
- Add end customers to organization and view messages assigned to them (enabled if you are running Service Now in the Partner Proxy mode).
- Run an organization in test mode and test connectivity of the organization with JSS.
- Export device data in CSV and Excel formats.
- Export inventory information in CSV format.
- Configure global settings (SNMP server and core file upload).
- Configure BIOS and product health data collection
- Configure system log file and request support information (RSI) collection

**Related
Documentation**

- [Junos Space Service Now Overview on page 48](#)
- [Service Now Modes](#)
- [Organizations Overview on page 93](#)
- [Device Groups Overview on page 105](#)
- [Devices Overview on page 108](#)
- [Event Profiles Overview on page 177](#)
- [AI-Scripts Overview on page 27](#)
- [Auto Submit Policy Overview on page 210](#)
- [Global Settings Overview](#)

Organizations

- [Organizations Overview on page 93](#)
- [Creating Organizations on page 95](#)

- [Modifying Organization Parameters on page 100](#)
- [Deleting an Organization on page 101](#)
- [Testing the Connection to JSS on page 102](#)
- [Viewing Messages Assigned to an End Customer on page 103](#)
- [Running an Organization in Test Mode on page 103](#)
- [Updating Core File Upload Configuration for an End Customer on page 104](#)

Organizations Overview

An organization in Service Now represents a unique site ID in the Customer Relationship Manager (CRM) of the Juniper Support System (JSS). JSS identifies a Service Now application by using the site ID of the organization configured on the Service Now application. An organization is configured on Service Now by providing a site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks or by a Service Now partner (in case of end-customer Service Now installation). When Service Now submits incidents for creating cases, the cases are created and associated with the site ID of the organization configured on Service Now.

A Service Now partner can manage multiple organizations using a single Service Now installation. This is done by dividing the network into multiple logical customer sites and assigning each customer site to an organization. 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 105](#).

For more information about creating device groups, see [“Creating a Device Group” on page 105](#).

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 8 on page 94](#).

Figure 8: 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@exam...	Success

Table 11 on page 94 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
Site ID	Identifier for the Customer Site in the Customer Relationship Manager (CRM) of JSS
Submit Cases As	<p>Specifies if the cases from a production environment should be submitted to JSS as a real case or a test case</p> <p>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.</p>
User Name	<p>User name to identify the user for communications with the JSS while creating cases or checking for updates</p> <p>You do not need to enter a user name or password if Service Now is in the offline mode.</p>
Connection Status	Status of the connection between the Service Now and JSS or Service Now partner
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)	

On the Organizations page, you can perform the following actions:

- Add an organization to Service Now; see [“Adding an Organization to Service Now”](#) on page 95 for details.
- Add an end customer to a Service Now partner; see [“Adding an End Customer to Service Now Configured in Partner Proxy Mode”](#) on page 98 for details.

- Modify the parameters of an organization; see [“Modifying Organization Parameters” on page 100](#) for details.
- Configure an organization to submit cases as test case; see [“Running an Organization in Test Mode” on page 103](#) for details.
- Test connectivity to JSS or Service Now partner; see [“Testing the Connection to JSS” on page 102](#) for details.
- Delete an organization from Service Now; see [“Deleting an Organization” on page 101](#) for details.
- Associate an organization with an address group; see [“Associating Devices with an Address Group From the Organizations Page” on page 224](#) for details.
- Update core-file upload configuration for a Service Now end customer; see [“Updating Core File Upload Configuration for an End Customer” on page 104](#) for details.



NOTE: This action is available only for an end customer on a Service Now partner setup.

- View messages assigned to end customers; see [“Viewing Messages Assigned to an End Customer” on page 103](#) for details.



NOTE: This action is available only for an end customer on a Service Now partner setup.

Related Documentation

- *Service Now Modes*
- *Junos Space Service Now Global Settings Overview*
- [Device Groups Overview on page 105](#)
- [Address Group Overview on page 220](#)

Creating Organizations

As part of the initial setup, you need to add an organization using the credentials that you have received with your license. If you are a Service Now partner, you can add one or more connected members and manage them. You can add end customers only after you add an organization.

- [Adding an Organization to Service Now on page 95](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 98](#)

Adding an Organization to Service Now

An organization in Service Now represents a unique site ID in the Customer Relationship Manager (CRM) of Juniper Support Systems (JSS). JSS identifies a Service Now application by using the site ID of the organization configured on the Service Now application. An organization is configured on Service Now by providing a site ID and

credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks for operating Service Now in Direct and Partner Proxy modes. For operating Service Now in End Customer mode, the Service Now partner provides the username and password to configure an organization.

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

To add a Service Now organization:

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

The **Add Organization** dialog box appears.

Figure 9: 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 96](#).

Table 12: Description of Fields on the Add Organization Page

Name	Description	Range/Length	Default
Name	Name of the organization	maximum 64 characters are allowed.	
Submit cases as	Specifies if the cases from this organization is to be submitted as real case or test case. The synopsis of a test case sent to JSS is appended with [Test Mode].	The values are: <ul style="list-style-type: none"> • Real cases • Test cases 	Real Cases

Table 12: Description of Fields on the Add Organization Page (*continued*)

Name	Description	Range/Length	Default
User Name	<p>Name used to identify the user in JSS while creating cases, and checking for updates to existing cases.</p> <p>You do not need to enter a user name or password if Service Now is in the Offline mode.</p>	<p>128 characters; should be in the e-mail address format.</p> <p>Characters can include alphabets, numbers, and the following special characters: ., -, _ and +.</p>	
User Password	<p>Password for the username required for communicating with JSS or Service Now partner.</p> <p>You do not need to enter a user name or password if Service Now is in the Offline mode.</p>	32 characters	
Get Sites (button)	<p>Identifier of the Customer Site in the Customer Relationship Manager(CRM) of JSS.</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>	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 IP addresses overwritten by asterisks Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information 	—	Send all information with IP addresses overwritten



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

3. Click **Submit**.

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

To add a Service Now organization in End Customer mode:

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

The Add Organization dialog box appears.

2. Enter the organization parameters in the provided fields.
For a detailed description of these fields, see [Table 12 on page 96](#).
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.

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

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



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

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

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

The **Add Member** dialog box appears as shown in [Figure 10 on page 99](#).

Figure 10: Add Member Dialog Box

Add Member

Name:

User Name:

User Password:

Confirm User Password:

JMB Filter Level: Send all information with IP addresses overwritten ▼

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

Page 1 of 1 Displaying 1 - 3 of 3

Submit **Cancel**

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

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

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

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

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

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

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

- **Do not send**—Prevents sending JMBs to JSS
 - **Send all information except configuration**—Sends all device information in a JMB except the device configuration information
 - **Send all information with IP Addresses overwritten**—Sends all the device information; however, the IP addresses associated with the device are overwritten with asterisks (*)
 - **Send all information**—Sends all the device information
 - **Only send list of features used**—Sends parameters configured without values assigned to the parameters
7. (Optional) Under **Select Configuration**, do one of the following:
- Select **Override Address** to override address group associated with end-customer devices. Overriding address groups of end customers allows a Service Now partner to send Return Materials Authorization (RMA) incidents of an end customer to JSS using the ship-to address associated with the device by the Service Now partner.
 - Select **Accept BIOS Validations** to accept BIOS data from the Service Now end customer for validation.
- If you do not select this check box, the **Configure BIOS Validation** option on the Actions menu of Service Now devices is disabled on the Service Now end customer.
- Select **Accept AIS Health Check Incidents** to accept AI-Scripts health check incidents from the Service Now end customer.
8. Click **Submit**.

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

**Related
Documentation**

- *Service Now Modes*
- [Organizations Overview on page 93](#)
- *Troubleshooting Issues with Adding an Organization to Junos Space Service Now*
- [Running an Organization in Test Mode on page 103](#)

Modifying Organization Parameters

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



NOTE: A Service Now partner cannot modify the name assigned to end-customer organizations.

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. For details about organization parameters, see [“Description of Fields on the Add Organization Page” on page 95](#).

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 93](#)
- [Deleting an Organization on page 101](#)
- [Running an Organization in Test Mode on page 103](#)

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 end customers associated with it.

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 93](#)
 - [Adding an Organization to Service Now on page 95](#)
 - [Running an Organization in Test Mode on page 103](#)

Testing 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:

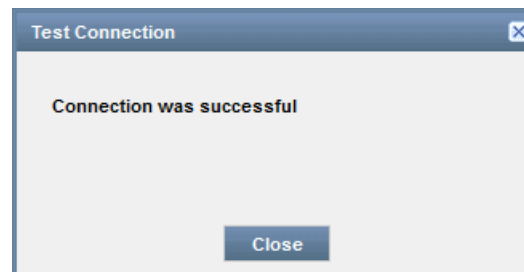
1. From the Service Now navigation tree, select **Administration > Organizations**.

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 11: 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 is operating in the Offline mode.

- Related Documentation**
- [Organizations Overview on page 93](#)
 - [Adding an Organization to Service Now on page 95](#)
 - [Deleting an Organization on page 101](#)
 - [Running an Organization in Test Mode on page 103](#)

Viewing Messages Assigned to an End Customer

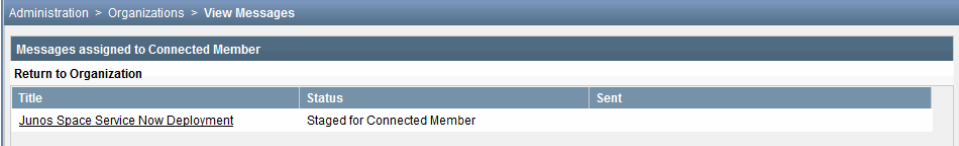
A Service Now partner can view the list of messages that are assigned to an end customer (also known as a connected member). This action is available only when Service Now operates in the Partner Proxy mode and when you select an end customer in the Organizations page.

To view the messages assigned to an end customer:

1. From the Service Now navigation tree, select **Administration > Organizations**.
The Organizations page displays the list of organizations and connected members.
2. Select the end customer 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 12 on page 103](#), the Messages assigned to Connected Member page displays the list of messages assigned to the selected end customer.

Figure 12: 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 an End Customer on page 262](#)
- [Messages Overview on page 259](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 98](#)

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 incidents submitted for testing purposes.

**Related
Documentation**

- [Organizations Overview on page 93](#)
- [Modifying Organization Parameters on page 100](#)

Updating Core File Upload Configuration for an End Customer

You can update the core file configuration for a Service Now end customer in Partner Proxy mode. If a Service Now partner is unable to configure a server for end customers to upload core files, end customers can upload core files server used by the Service Now partner. For more details, see [“Uploading Core Files Generated for Events” on page 208](#).

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 Upload Core File Upload configuration is successfully changed.

**Related
Documentation**

- [Organizations Overview on page 93](#)
- [Viewing Messages Assigned to an End Customer on page 103](#)

Device Groups

- [Device Groups Overview on page 105](#)
- [Creating a Device Group on page 105](#)

- [Modifying a Device Group on page 107](#)
- [Deleting a Device Group on page 107](#)

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 assign devices to it; see [“Creating a Device Group” on page 105](#) for details.
- Modify device groups; see [“Modifying a Device Group” on page 107](#) for details.
- Delete device groups; see [“Deleting a Device Group” on page 107](#) for details.
- Associate address groups; see [“Associating Devices with an Address Group from the Device Groups Page” on page 225](#) for details.
- Set default device group
- Assign the device group to another domain; see [“Assigning a Service Now Object to a Domain” on page 50](#) for details.

Related Documentation

- [Service Now Devices Overview on page 108](#)
- [Organizations Overview on page 93](#)
- [Address Group Overview on page 220](#)

Creating a Device Group

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

Device Group in Direct mode:

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

Device Group in Partner Proxy Mode:

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

To create a device group:

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

The Create Device Group page appears.

Figure 13: Create Device Group Page

2. Enter a name for the device group within the **Name** field.
The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-). The maximum number of characters allowed is 64.
3. In the **Organizations** list, select an organization for this device group.
If you want to associate the device group with a new organization, click **New Organization** and configure an organization. See [“Adding an Organization to Service Now” on page 95](#) for configure an organization.
4. Select the devices that you want to add to this device group from the **Select Device to add them to the Device Group** section.
5. Click **Add**.

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

- Related Documentation**
- [Device Groups Overview on page 105](#)
 - [Modifying a Device Group on page 107](#)
 - [Service Now Devices Overview on page 108](#)
 - [Installing AI-Scripts on a Device](#)

Modifying a Device Group

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 as follows—**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 105](#)
 - [Deleting a Device Group on page 107](#)
 - [Creating a Device Group on page 105](#)

Deleting a Device Group

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 105](#)
- [Creating a Device Group on page 105](#)

Service Now Devices

- [Junos Space Service Now Devices Overview on page 108](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Uninstalling an Event Profile from a Device on page 117](#)
- [Exporting Device Data in CSV and Excel Formats on page 119](#)
- [Exporting Inventory Information in CSV Format on page 119](#)
- [Viewing Exposure to Known Issues on page 120](#)
- [Generating an On-Demand Incident on page 121](#)
- [Collecting RSI and System Log Files on page 124](#)
- [Requesting an RMA Incident on Service Now on page 127](#)
- [Moving a Device to Maintenance Mode on page 130](#)
- [Deleting a Device from Junos Space Service Now on page 131](#)
- [Associating Devices with a Device Group on page 132](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)
- [Viewing Incidents on page 134](#)
- [Verifying the Connection Between a Device and the FTP Server on page 135](#)
- [Service Now End Customer–Partner Communication Overview on page 135](#)
- [Installing the SSL Certificate on a Service Now End Customer on page 140](#)

Junos Space Service Now Devices Overview

For Junos Space Service Now to monitor and detect events on devices, you must discover the devices using the Junos Space Network Management Platform, add the devices to Service Now, and then install AI-Scripts on the devices.

You can view only those devices discovered by the Junos Space Platform for which you have permission (based on the role-based access control [RBAC] policy). When you add a device to Service Now, you receive informational JMB (iJMBs) and event JMBs (eJMBs) that help you monitor and resolve issues on the device.

You can group multiple devices into a single device group so that you can manage these devices as a single entity; for example, you can install or uninstall AI-Scripts on all the devices in a device group in a single operation.

You can view Service Now devices on the Service Now devices page. Double-click a device to view its details. Details about the device are displayed under the following four tabs—Details, Address Details, Contract Details, and Device Analysis.

- Details—Provides general details such as the hostname, IP Address, and serial number of the device
- Address Details—Provides the ship-to-address and location where the device is present
- Contract Details—Provides service contract details of a device



NOTE: Service Now populates the details of the start and end dates of contract and end-of-life (EOL) information of the device components on the View Physical Inventory page of the Junos Space Network Management Platform GUI. For details about accessing the View Physical Inventory page, see [Viewing Physical Inventory](#).

- Device Analysis—Provides details such as the Routing Engine, and time and status of the data collected from the device for validating the BIOS integrity of the device

[Table 13 on page 109](#) describes the attributes of Service Now devices displayed under the four tabs.

Table 13: Service Now Devices Field Descriptions


Field Name	Description
Details tab	
Organization	Name of the organization to which the device is assigned
Connected Member	Name of the connected member
Device Group	Name of the device group to which the 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
Platform	Model of the device
OS Version	Version of the Junos OS that is running on the device

Table 13: Service Now Devices Field Descriptions (*continued*)

Field Name	Description
State	By default, this field is hidden. This field is displayed only for end-customer devices in a Service Now application operating in the 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
Routing Engine	Type of Routing Engine present on the device; the values are: <ul style="list-style-type: none"> • Single Routing Engine • Dual Routing Engines
Domain	Domain to which the device is assigned.
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
Policy	Autosubmit policies associated with the device for submitting incidents to a Service Now partner (for Service Now operating in End Customer mode) or Juniper Support Systems; each policy is separated by a comma.
RSI File Collection	Configuration for collecting RSI from the device
BIOS File Collection	Configuration for collecting BIOS files from the device
Log File Collection	Configuration for collecting system log files from the device
Connection Status	Status of connection between the device and Service Now
Maintenance Mode	Specifies whether the device is currently in maintenance mode or not. Possible values are: <ul style="list-style-type: none"> • ON: The device is in maintenance mode. • OFF: The device is not in maintenance mode.
Alerts	Status of iJMB received from the device
Support Contract Information	Table to display information about the support contract for the device. The following fields are included in the table: contract number, status, SKU, SKU type, as well as start and end dates of the contract. To receive on-demand updates about your Service Now contract, click the Refresh button on the Device Details page.

Table 13: Service Now Devices Field Descriptions (*continued*)

Field Name	Description
Address Details tab	
Ship-to Address	Address to which the device or device parts should be shipped
Location	Location the device is installed
Contract Details tab	
Contract #	Service contract number of the device
Status	Status of the device service contract
SKU	Stock-keeping unit of the device
SKU Type	Type of SKU of the device
Start Date	Start date of the device service contract
End Date	End date of the device service contract
Device Analysis tab	
Entity	Routing Engine from which data was collected for BIOS validation
Type	Type of device analysis
Last Collected	Date and time when the data was last collected for BIOS validation
Status	<p>Status of BIOS validation:</p> <ul style="list-style-type: none"> • Pending Submission—Service Now has received data for BIOS validation from the device; the data is yet to be submitted to Juniper Support System (JSS). • Pending Case Creation—BIOS validation data of the device is received by JSS; JSS is yet to create a case for the received data. • Case Created—JSS has created a case for the BIOS validation data received for the device. <p>NOTE: This field is not applicable if Service Now is operating in the End Customer mode.</p> <ul style="list-style-type: none"> • Case Creation Failed—JSS failed to create a case for the BIOS validation data received for the device. <p>NOTE: This field is not applicable if Service Now is operating in the End Customer mode.</p> <ul style="list-style-type: none"> • Submission Failed—Service Now is unable to submit the BIOS validation data of the device to JSS. • Validation Success—The validation of BIOS data of the device by JSS was successful. • Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.

The  icon, if displayed in the row of a device on the Service Now Devices page, indicates one of the following scenarios:

- There is a mismatch between the versions of AI-Scripts installed on a device and AI-Scripts bundle present on Service Now.

This icon is also displayed 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 AI-Scripts version installed on a device—for example, when you add a device to Service Now that already has AI-Scripts installed on it.
- After installing AI-Scripts on a device by using Service Now, you have manually deleted AI-Scripts from the device.
- One or more JMB files, attachments, and log files are not deleted from a device after these files are copied from the device to Service Now.

If you place the cursor on the icon, a 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 names 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 Junos Space Platform to Service Now; see [“Adding Devices to Junos Space Service Now” on page 114](#) for details.
- Install event profiles on the devices; see [“Installing an Event Profile on a Device by Using Service Now” on page 114](#) for details.
- from the devices; see [“Uninstalling an Event Profile from a Device” on page 117](#) for details.

- Configure BIOS validation; see [“Configuring BIOS Validation for Verifying BIOS Integrity of a Device” on page 145](#) for details.
- Configure product health data collection (PHDC); see [“Configuring Product Health Data Collection on a Device” on page 155](#) for details.
- Export device data in CSV and Excel formats; see [“Exporting Device Data in CSV and Excel Formats” on page 119](#) for details.
- Delete devices from Service Now; see [“Deleting a Device from Junos Space Service Now” on page 131](#) for details.
- Associate devices with a device group; see [“Associating Devices with a Device Group” on page 132](#) for details.
- Associate auto submit policies with devices; see [“Assigning an Auto Submit Policy to a Device” on page 133](#) for details.
- Export inventory information in CSV format; see [“Exporting Inventory Information in CSV Format” on page 119](#) for details.
- View the devices that are susceptible to known issues; see [“Viewing Exposure to Known Issues” on page 120](#) for details.
- Generate on-demand incidents; see [“Generating an On-Demand Incident” on page 121](#) for details.
- Request RMA incidents; see [“Requesting an RMA Incident on Service Now” on page 127](#) for details.
- Associate devices with an address group; see [“Associating Devices with an Address Group from the Service Now Devices Page” on page 226](#) for details.
- Verify the connection between the devices and the FTP server; see [“Verifying the Connection Between a Device and the FTP Server” on page 135](#) for details.
- View incidents created on the device; see [“Viewing Incidents” on page 134](#) for details.
- Configure RSI and log file collections; see [“Collecting RSI and System Log Files” on page 124](#) for details.
- Assign a device to another domain; see [“Assigning a Service Now Object to a Domain” on page 50](#) for details.
- Move a device to maintenance mode; see [“Moving a Device to Maintenance Mode” on page 130](#) for details.

**Related
Documentation**

- [Device Groups Overview on page 105](#)
- [Event Profiles Overview on page 177](#)
- [Auto Submit Policy Overview on page 210](#)
- [BIOS Validation Overview on page 141](#)
- [Product Health Data Collection Configuration Overview on page 153](#)
- [Incidents Overview on page 232](#)

Adding Devices to Junos Space Service Now

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

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 are discovered by Junos Space Platform, but not added to Service Now.

Figure 14: 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	xxxxxxxxxx	ACX2000	12.3-20130929_acx_x51_s1.0

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

The Service Now Device(s) page appears and lists the devices added to Service Now..

Related Documentation

- [Junos Space Service Now Devices Overview on page 108](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)

Installing an Event Profile on a Device by Using Service Now


An event profile defines a set of event scripts selected from an AI-Scripts bundle for which Juniper Message Bundles (JMBs) are generated to notify users about an event when the event occurs on a device running Junos OS. When you install an event profile on managed devices, the event scripts provide the information needed to automatically detect and report problem (incident), 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 devices with dual Routing Engines, Service Now installs the event profile on both primary and backup Routing Engines.



NOTE: A Service Now partner cannot install event profiles on a Service Now end-customer's devices.

The  icon appears against a device on the Service Now Devices 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 a message similar to the following message:

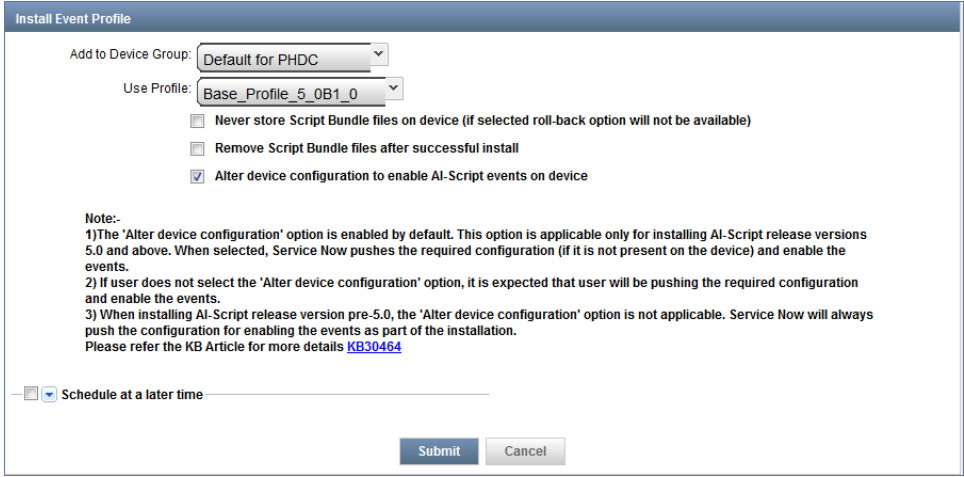
There is a mismatch of the AI-Scripts installed on *routing engine* on *device*.

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. The Install Event Profile action is active even if the devices are not associated with an organization or Device Group.
3. From the Actions menu, select **Device Operations > Install Event Profile**. Alternatively, right-click the device and select **Device Operations > Install Event Profile**.

The Install Event Profile page appears as shown in [Figure 15 on page 115](#).

Figure 15: Install Event Profile Page



Install Event Profile

Add to Device Group: Default for PHDC

Use Profile: Base_Profile_5_0B1_0

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

☐ Remove Script Bundle files after successful install

☒ Alter device configuration to enable AI-Script events on device

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

☐ Schedule at a later time

Submit **Cancel**

4. Select the appropriate Device Group from the **Add to Device Group** drop-down list to add the device to.
5. Select an event profile from the **Use Profile** drop-down list to assign to the device.

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.



NOTE: This option is not available during the installation of event profiles on the QFX3000-M, QFX3000-G and EX Series devices with dual Routing Engines.

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: This option is not available during the installation of event profiles on QFX3000-M, QFX3000-G, and EX Series devices with dual Routing Engines.

8. (Optional) if you do not want the device configuration to be modified while committing the event profile on the device, clear the **Alter device configuration to enable AI-Script events on device** check box.

By default, this option is selected.



NOTE:

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

9. (Optional) If you want to schedule a time for installing the event profile, 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.
10. Click **Submit**.
11. (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.
12. Click **Finish**.

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

13. Do one of the following: Click one of the following links based on the required results.

- Apply the event profile to devices manually.

To apply the event profile to devices manually:

- a. Click the **Apply this Event Profile to Devices manually** link.
- b. Click the devices on which you want to apply the event profile.
- c. 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. The Jobs page displays the status of the job. Double-click the job to view information about each step of the installation.

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

- Return to the Event Profiles page

Click **Return to the Event Profiles Page** to return to the Event Profiles page.

Related Documentation

- [Event Profiles Overview on page 177](#)
- [AI-Scripts Overview on page 27](#)
- [Manually Installing AI-Scripts on Devices on page 39](#)
- [Adding a Script Bundle to Junos Space Service Now on page 200](#)
- [Viewing Exposure to Known Issues on page 120](#)

Uninstalling an Event Profile from a Device

You can use Service Now to uninstall event profiles from managed 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 uninstall event profiles from devices. DMI is an extension to the NETCONF network management protocol.



NOTE: A Service Now partner cannot uninstall event profiles from a Service Now end-customer's devices.

To uninstall event profiles from a managed device:

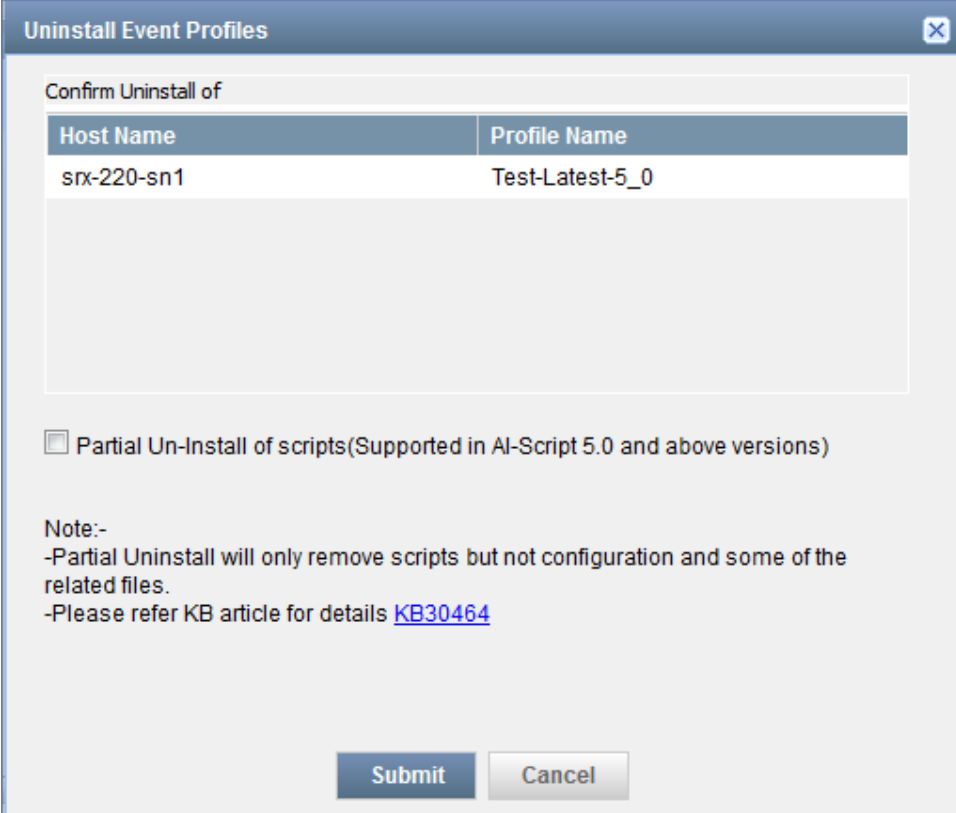
1. From the Service Now navigation tree, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the device from which you want to uninstall the event profile.
3. From the Actions menu, select **Device Operations > Uninstall Event Profile**. Alternatively, right-click the device and select **Device Operations > Uninstall Event Profile**.

The Uninstall Event Profile dialog box appears as shown in [Figure 16 on page 118](#).

Figure 16: Uninstall Event Profiles Dialog Box



The dialog box is titled "Uninstall Event Profiles" and contains a table for confirming the uninstall of an event profile. Below the table is a checkbox for "Partial Un-Install of scripts" and a note section. At the bottom are "Submit" and "Cancel" buttons.

Host Name	Profile Name
srx-220-sn1	Test-Latest-5_0

☐ Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)

Note:-
 -Partial Uninstall will only remove scripts but not configuration and some of the related files.
 -Please refer KB article for details [KB30464](#)

Submit **Cancel**

4. Select the **Partial Un-install of scripts(Supported in AI-Script 5.0 and above versions)** to avoid the AI-Scripts configuration from being modified when uninstalling the event profile from the device.



NOTE: If you uninstall AI-Scripts Release 5.0 or later with the **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** option cleared, ensure that the AI-Scripts configuration is deleted manually by executing the `/var/db/scripts/remove-jais.slax` script to avoid errors while committing the next AI-Scripts configuration (during installation or upgrade).

5. Click **Submit**. A job to uninstall the event profile is initiated.

Click the *job ID* link to view the status of the job.

Related Documentation

- [AI-Scripts Overview on page 27](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Manually Installing AI-Scripts on Devices on page 39](#)

Exporting Device Data in CSV and Excel Formats

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

- [Junos Space Service Now Devices Overview on page 108](#)
- [Deleting a Device from Junos Space Service Now on page 131](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)

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

- [Junos Space Service Now Devices Overview on page 108](#)
- [Deleting a Device from Junos Space Service Now on page 131](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)
- [Viewing Exposure to Known Issues on page 120](#)

Viewing Exposure to Known Issues

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

- [Junos Space Service Now Devices Overview on page 108](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Deleting a Device from Junos Space Service Now on page 131](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)

- [Collecting RSI and System Log Files on page 124](#)

Generating an On-Demand Incident

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. On-demand JMBs can be generated by AI-scripts installed on devices or by Service Now. The on-demand JMBs generated by Service Now are referred to as off-box on-demand JMBs.

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 System (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.

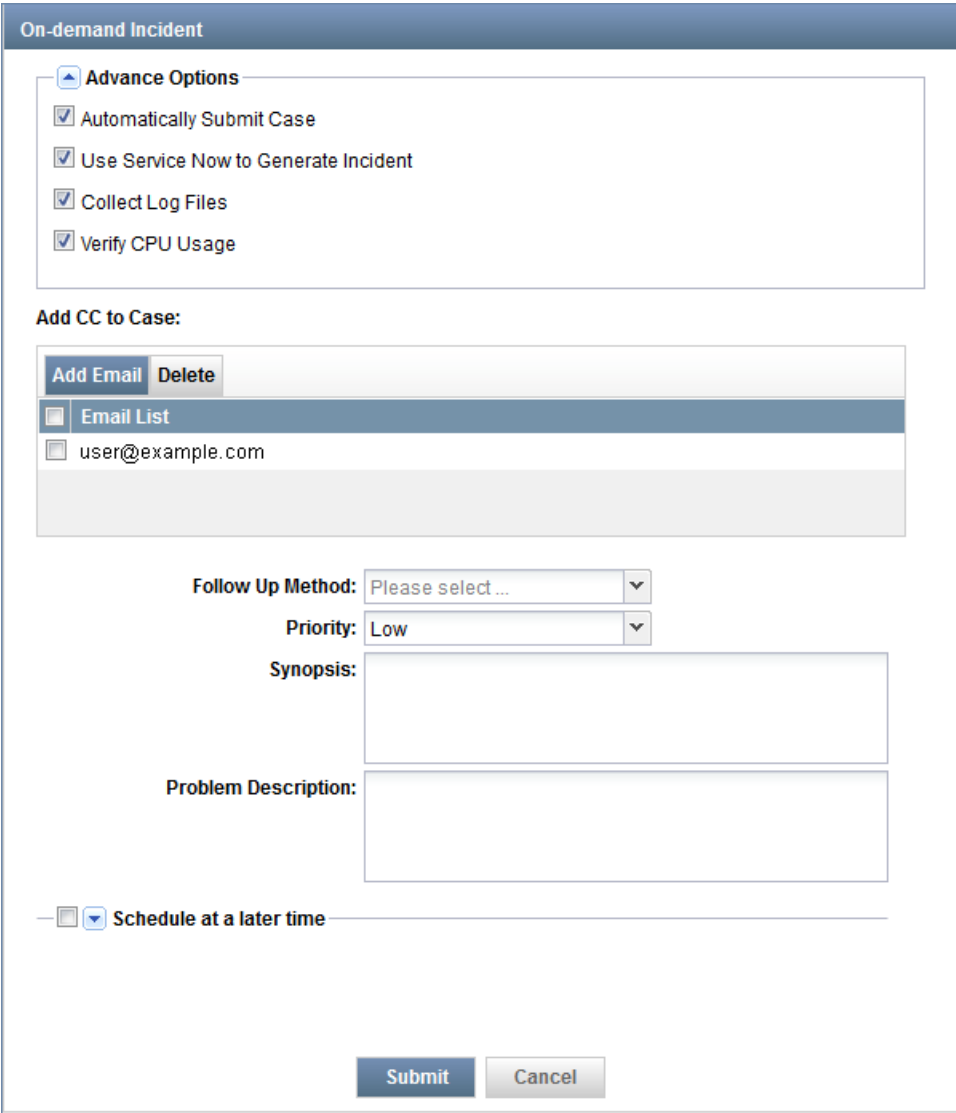
To generate an on-demand incident:

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 **Device Operations > 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 17 on page 122](#).

Figure 17: On-demand Incident Dialog Box



The dialog box is titled "On-demand Incident". It contains several sections:

- Advance Options:** A section with four checked checkboxes:
 - ☒ Automatically Submit Case
 - ☒ Use Service Now to Generate Incident
 - ☒ Collect Log Files
 - ☒ Verify CPU Usage
- Add CC to Case:** A section with two buttons, "Add Email" and "Delete", and a list box labeled "Email List". The list box contains one entry: "user@example.com".
- Follow Up Method:** A dropdown menu with the text "Please select ...".
- Priority:** A dropdown menu with the text "Low".
- Synopsis:** A text input field.
- Problem Description:** A text input field.
- Schedule at a later time:** A checkbox that is currently unchecked.
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

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.

Selecting the **Use Service Now to Generate Incident** check box displays the following options:

- a. **Collect Log Files:** Specifies if log files should be collected for the JMB.

By default, the check box is selected and log files are collected for an off-box on-demand JMB. Clear the check box to avoid collecting log files for off-box on-demand JMBs.

- b. **Verify CPU Usage:** Specifies if load average values and ideal time of the CPU should be checked before generating the off-box on-demand JMB.

By default, this check box is selected. If the average load and ideal time of the CPU are not within the limits defined in [Table 14 on page 123](#), the off-box on-demand JMB is not generated and an error message is displayed. Service Now determines the CPU load average from the output of the **get-system-uptime-information** command and the CPU idle time from the output of the **get-route-engine-information** command.

Table 14: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs

Device	CPU Load Average	CPU Ideal Time
MX240, MX480, MX960, MX120, MX320	< 2	> 15
Other Supported Devices	< 1	> 15

6. Under Email List, click 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** buttons 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 step 6 through step 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 that appears displays the job ID as a link.

You can click the job ID link 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 18 on page 124](#)), which displays information about the job such as the profile used in the incident, hostname of the device running Junos OS, job status, and reason for the incident.

Figure 18: Create On-demand Incident Status Dialog Box

Profile Name	Host Name	Status	Reason
General	ex-4200-sn4	Failed	OP Script execution failed on device 688250. Src File: on-demand.slax Please verify that the AI Script with version 3.2R1 or higher is installed on device.

Message from device : Details: Operational RPC Command Results
Failed to open netconf channel domainId=0 deviceId=688250

Page 1 of 1 | Displaying 1 - 1 of 1

Related Documentation

- [Junos Space Service Now Devices Overview on page 108](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Deleting a Device from Junos Space Service Now on page 131](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)
- [Viewing Exposure to Known Issues on page 120](#)
- [Collecting RSI and System Log Files on page 124](#)

Collecting RSI and System Log Files

Service Now provides the Configure File Collections option to configure the interval during which a Request Support Information (RSI) command can be executed on a device to gather device configuration information. For example, you can set the RSI command to be executed every two hours. When you configure an interval for collecting RSI, Service Now executes the RSI command only once during the configured interval to collect RSI. For events that occur after RSI is collected, RSI is not collected if the event occurs within the configured interval.


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

- Configured interval for collecting RSI: 1hr

- Time at which RSI was last executed: 1:00 PM

Time of Event	RSI Executed	Comment
1:30 PM	No	RSI is not collected at 1:30 PM as one hour has not yet elapsed since RSI was last collected at 1:00 PM.
1:59 PM	No	RSI is not collected at 1:59 PM as one hour has not yet elapsed since RSI was last collected at 1:00 PM.
2:00 PM	Yes	RSI is collected at 2:00 PM as one hour has elapsed since RSI was last collected at 1:00 PM.
2:01 PM	No	RSI is not collected at 2:01 PM as one hour has not yet elapsed since RSI was last collected at 1:00 PM.
4:30 PM	Yes	RSI is collected at 4:30 PM as two-and-a-half hours have elapsed since RSI was last collected at 2:00 PM. The configured interval to collect RSI is 1hr.
4:35 PM	No	RSI is not collected at 4:35 PM as one hour has not yet elapsed since RSI was last collected at 4:30 PM.
5:30 PM	Yes	RSI is collected at 5:30 PM as one hour has elapsed since RSI was last collected at 4:30 PM.



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-Scripts 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 Configure File Collections dialog box appears as shown in [Figure 19 on page 126](#).

Figure 19: Configure File Collections Dialog Box

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 on page 27](#)

Requesting an RMA Incident on Service Now

You can use the Off-Box feature in Service Now to request Return Materials Authorization (RMA) incidents for a device. With the Off-Box feature, Service Now generates RMA incidents using the preloaded **directive.rc** file. 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 end customers.

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 **Device Operations > 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 20 on page 128](#).

Figure 20: 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 Juniper Support Systems (JSS).
5. (Optional) Clear the **Collect Log Files** check box if you do not want to collect log files for the RMA JMBs.
6. (Optional) Clear the **Verify CPU Usage** if you do not want load average values and ideal time of the CPU to be checked before generating the Request RMA JMBs.

If the average load and ideal time of the CPU are not within the limits defined in [Table 15 on page 129](#), the RMA JMBs are not generated and an error message is displayed. Service Now determines the CPU load average from the output of the

get-system-uptime-information command and the CPU idle time from the output of the **get-route-engine-information** command.

Table 15: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs

Device	CPU Load Average	CPU Ideal Time
MX240, MX480, MX960, MX120, MX320	< 2	> 15
Other Supported Devices	< 1	> 15

7. Under Email List, click the **Enter Email Id** check box to enter an e-mail ID in the user@example.com format.
8. (Optional) To add or delete e-mail IDs, use the Add Email or Delete buttons respectively.
9. 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.
10. From the **Priority** list, select the priority of the case.
The available options are—Critical, High, Medium, and Low. The default priority is Low.
11. In the **Synopsis** field, enter a synopsis of the RMA incident.
The maximum number of characters allowed in the Synopsis field is 1028 characters.
12. 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.
13. 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.
14. Enter the address in the **Ship-to Address** field to which the device components or parts must be shipped.
15. 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.
16. (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.
17. 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 an On-Demand Incident on page 121](#)
 - [Junos Space Service Now Devices Overview on page 108](#)
 - [Collecting RSI and System Log Files on page 124](#)

Moving a Device to Maintenance Mode

Junos Space Service Now provides the *Maintenance Mode* option on the Actions menu to move a managed device to the maintenance mode. When a device is placed in the maintenance mode, event Juniper Message Bundles (eJMBs) are not generated on the device.

You cannot perform the following when a managed device is placed in maintenance mode:

- Configure BIOS validation
- Configure product health checks
- Generate on-demand JMBs (on-box, using AI-Scripts)
- Generate on-demand device snapshots

If Service Now is operating in the End Customer mode, it provides updates to the Service Now partner about the Service Now devices in maintenance mode once a day or whenever a device is moved to or out of the maintenance mode. A Service Now partner can view whether managed devices of Service Now end customers are in maintenance mode or not, but cannot move the devices of Service Now end customers to maintenance mode.



NOTE: Devices can be moved to maintenance mode only if AI-Scripts Release 5.0 or later is installed on the device.



NOTE: QFX Series devices in a QFabric cannot be moved to the maintenance mode.

To move a device to maintenance mode:

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 that you want to move to maintenance mode.
3. From the Actions menu, select **Device Operations > Maintenance Mode**. Alternatively, right-click the device and select **Device Operations > Maintenance Mode**.

The Configure Maintenance Mode dialog box appears as shown in [Figure 21 on page 131](#).

Figure 21: Configure Maintenance Mode Dialog Box

4. On the Configure Maintenance Mode dialog box, do one of the following:
 - Click **Enable Maintenance Mode** to move the device to maintenance mode.
 - Click **Disable Maintenance Mode** to move the device out of maintenance mode.
5. From the **Apply to** drop-down list, do one of the following:
 - Select **Selected device(s)** to move devices selected on the Service Now Devices page to the maintenance mode
 - Select **All managed devices in the current domain** to move all the managed devices in the current domain to maintenance mode.
6. Select the **Schedule Device Maintenance Mode at Specified Time** to schedule the time to move devices to the maintenance mode.
7. Click **Submit** to move the device to the maintenance mode.
The progress of the job to move the devices to the maintenance mode is displayed.
8. (Optional) Click the **job id** link to view the progress of the job.
After the device is moved to maintenance mode, the Service Now Devices page displays ON in the Maintenance Mode column of the device.

Deleting a Device from Junos Space Service Now

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

When you delete a device that has AI-Scripts installed on it from Service Now, the AI-Scripts are automatically uninstalled from the device.



NOTE: If you uninstall a device from the Junos Space Platform first, you need to manually uninstall AI-Scripts from the device.

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 one or more devices that you want to delete, and click **Delete** on the **Actions** menu. Alternatively, right-click the device and select **Delete**.

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

3. Select the **Delete device(s) even if AI-Scripts un-installation fails** check box to delete the device from Service Now even if the uninstallation of AI-Scripts fails on the device.

If you do not select this option, the device is not deleted from Service Now if the uninstallation of AI-Scripts fails on the device.

4. 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**

- [Junos Space Service Now Devices Overview on page 108](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Modifying a Device Group on page 107](#)

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 an edn customer in a single Service Now device group. Alternately, you can create a device group for each end customer and associate them to Service Now organizations dedicated to each end customer. 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

- [Junos Space Service Now Devices Overview on page 108](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Modifying a Device Group on page 107](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)

Assigning an Auto Submit Policy to a Device

Auto submit policies enable devices to submit events that occur on them to Juniper Support System (JSS) automatically in the form of incidents. 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 211](#).

To assign an auto submit policy to a device:

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 22: 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 assigned to the auto submit policies.

Related Documentation

- [Auto Submit Policy Overview on page 210](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Junos Space Service Now Devices Overview on page 108](#)
- [Collecting RSI and System Log Files on page 124](#)

Viewing Incidents

Incidents are created on Service Now when an event occurs on the device.

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. For information about incident details, see “[Viewing Incident Details](#)” on page 244.

Related Documentation

- [Junos Space Service Now Devices Overview on page 108](#)
- [Adding Devices to Junos Space Service Now on page 114](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Modifying a Device Group on page 107](#)
- [Collecting RSI and System Log Files on page 124](#)

Verifying the Connection Between a Device and the 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

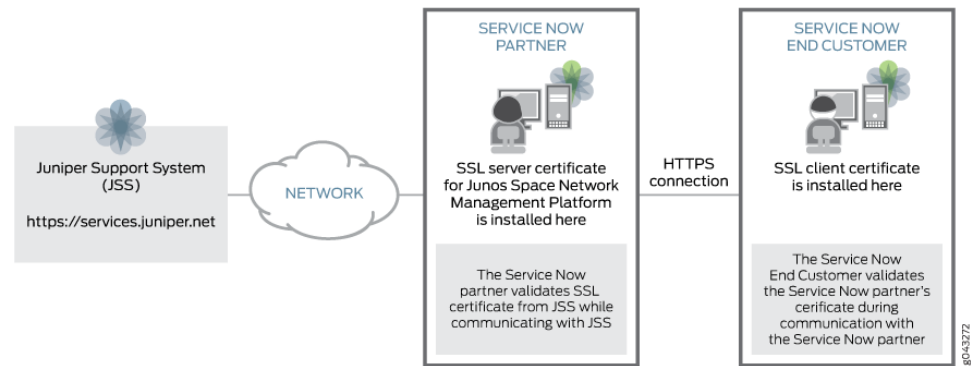
- [Junos Space Service Now Devices Overview on page 108](#)
- [Uploading Core Files Generated for Events on page 208](#)
- [Updating Core File Upload Configuration for an End Customer on page 104](#)

Service Now End Customer–Partner Communication Overview

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

Figure 23 on page 136 depicts the communication between a Service Now partner with a Service Now End Customer and Juniper Support System (JSS) using an SSL certificate.

Figure 23: Service Now Partner Communicating with a Service Now End Customer and JSS Using SSL Certificate



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

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

To secure the communication between a Service Now partner and Service Now End Customer, the following tasks must be performed:

1. [Generating CSR by Service Now Partner on page 136](#)
2. [Obtaining Signature of a Certificate Authority on page 138](#)
3. [Uploading the Certificate to Service Now Partner on page 139](#)
4. [Obtaining the Intermediate Certificate \(key\) for Establishing Credibility of the SSL Certificate on page 139](#)
5. [Obtaining SSL Certificate of the Service Now Partner on page 139](#)

Generating CSR by Service Now Partner

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

To generate a CSR:

1. Log in to the Junos Space Appliance.
The Junos Space Settings Menu Is displayed.
2. Type **7** if the Junos Space Appliance is a virtual appliance or type **6** if the Junos Space Appliance is a hardware appliance to access the SSH shell.
3. Change the directory to `/etc/pki/tls`.


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

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

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

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

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

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

7. Enter a pass phrase for the private key.

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

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

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

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

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

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

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

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

```
server $ cat server.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 019649A2E4BBCC4C

uKKzDLcMrBpuYDkxS16epQqoScvcYnJvTM5kaJKNnXVrUarYA16JYFsZB0EpqCjr
AV7Ln6hg8J1+UPEbrZPvXVED29qvM4tp1SDwKwuLs+IRWsON9ee2TsmVubCE0Ac7
aA8jg7kzubCktF3y+8/TM3yf+IWMy4EdWBXWtjMB022kjU5KGwyznQeCsN2HtOLp
WvFOFDQHgxougL0qfF7pkDsVby5bKv740T+ju/On6HtLf8IUfZDh/Xui/scsoKeb
8eJnNKN01dYAtU+eyNwkmP1o9j8Ly/Geei00amMFaDp01WuMQLmEH8En3tVIULrD
WZ2Ly0U9+d6J16f7LXXIEcBcH0e00C3pp7Bq4z1k0/2WPq5FmcM90mZZdeC2ZeYP
fNzBk21ZVVDAM89ggN1RNsm6FG9F6kkfczjB0SvawhBs7AgTDzty5J279uTGIyo1
1CVXbijo9+KR3INX3nWatYYR7T7MUG1Yma/MbCg2dWAPR6iwYwY3w6VD51BIGNCP
po42Y0H4yLvT80uVzpkQ8z9tjuk05ZAR6E8fWEdiYBbPIhfEBxc7WVUBdPE/OQaj
8FuyLnzY5iCxY1tkyWhtXntX32NrHJdJp6A8HFJf/v3ZnJ8FRHrNXtALcENVkgit
iCgmsGr5zwThiJqdSp6Xd4YpJrws5BaTGRNjOrhfunGyEebhYmsQVKZpuXYM/YuV
5/Nqd3Hdmx58hWxVi0Cm7+HU1RFRcu+JBhBLOJ9rBzaDVAFRqNtkMkF1wHKQ6u9K
1y+qg07gT8jYIWGFksB70QdMF+MntA+SvD5bfoUd6CY=
-----END RSA PRIVATE KEY-----
```

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

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

```
server $ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwFTELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UE
BxMGU31kbnV5MRAdDgYDVQQKEwdKdW5pcGVyMQswCQYDVQQLZWJBUzEPMA0GA1UE
AxMGaGUtbWUwMR8wHQYJKoZIhvcNAQkBFhBmcmVkbGp1bm1wZXIubmVOMIGfMA0G
CSqGSIb3DQEBAAQAA4GNADCBiQKBggQjA2megTM4/9iP9I56iNqmKmROQYfPwHLn
pW7Bwq1D1kzn8BqM6cFeMa1vUpRntiPJRNbUjGZPbfa3cwZEy/vgy3MyTALFj9Zy
7tkpUIId1Qn2KhW47mEcaixkEec5PxOUZm3Af1kKcMtIzajxyVRs6cr6xLy0Bqew
1TA+3Xj6PwIDAQABOskwFwYJKoZIhvcNAQkHMqoTCGZyZWQxMjM0M0A0GCSqGSIb3
DQEBBQUAA4GBAJjxApGFYAFfU11x0osdoGzedRkrVmR5693+h0EtI01n0z70NCVU
ix0in4dH0SDipNPgfZwQ0jx6wyVGx/b6wWpMxBTrvhxH1EiCgR9p0U63eMZsyEI
3RoU+7KeRTxtXbRYUx0EHGPD0HSgiShbjVc2uAPXijSR1utI3sViTJ2
-----END CERTIFICATE REQUEST-----
```

Obtaining Signature of a Certificate Authority

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



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

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

Uploading the Certificate to Service Now Partner

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

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

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

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

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

Obtaining SSL Certificate of the Service Now Partner

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



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

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

1. Open Mozilla Firefox Web browser and enter the URL to access the Service Now partner.
2. On the web browser, click the padlock present before the URL.

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

3. Click **More Information**.

The Page Info dialog box appears.

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

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

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

The Save To dialog box of the web browser appears.

6. Save the certificate on your local system.

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

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

1. Connect to the Virtual IP (VIP) node of the Junos Space cluster on which the Service Now partner is installed and configured.
2. Type **7** if the Junos Space Appliance is a virtual appliance or type **6** if the Junos Space Appliance is a hardware appliance to access the SSH shell.
3. Type the following from the command line:

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

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

Installing the SSL Certificate on a Service Now End Customer

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

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

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

The screenshot shows the 'Partner Certificate Configuration' page. At the top, there is a blue header with the title. Below the header, a message states: 'No Certificate is present. Please upload the certificate provided by the partner.' At the bottom of the message box, there are two buttons: 'Upload' and 'Close'.

2. Click **Upload**.

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

The screenshot shows the 'Partner Certificate Configuration' page after clicking 'Upload'. It features a 'Certificate' label followed by a text input field and a 'Browse...' button. At the bottom, there are 'Upload' and 'Close' buttons.

3. Click **Upload**.

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

The screenshot shows the 'Partner Certificate Configuration' window. It displays the following information:

- Subject Name:** EMAILADDRESS=root@192.0.2.166 CN=192.0.2.166 OU=Junos Space, O="Juniper Netw
- Issuer Name:** EMAILADDRESS=root@192.0.2.166 CN=192.0.2.166 , OU=Junos Space, O="Juniper Netw
- Signature Algorithm Name:** SHA1withRSA
- Serial Number:** 4933
- Not Before:** Fri Mar 27 05:38:58 UTC 2015
- Not After:** Thu Mar 26 05:38:58 UTC 2020

At the bottom of the window are two buttons: 'Delete Certificate' and 'Close'.

Related Documentation

- [Service Now End Customer–Partner Communication Overview on page 135](#)
- [Certificate Management Overview](#)

BIOS Validation

- [BIOS Validation Overview on page 141](#)
- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 145](#)

BIOS Validation Overview

Using Junos Space Service Now, you can analyze the BIOS image installed on a device running Junos OS and verify the integrity of the BIOS image. When you enable and configure BIOS validation on a device, AI-Scripts installed on the device collect the BIOS image data from the device. In response to the BIOS image data collected, BIOS validation incidents are created in Service Now and the collected BIOS data is submitted to Juniper Support System (JSS) to create a BIOS Health Check case. In response to the BIOS Health Check case, JSS validates the BIOS image data from the device and sends the validation result to Service Now.

A Service Now partner can accept or reject data for BIOS validation sent by a Service Now end customer. If a Service Now partner chooses to accept the data for BIOS validation from a Service Now end customer, the Service Now end customer submits the BIOS data to the Service Now partner which in turn submits the BIOS data to JSS for validation. If the Service Now partner chooses not to accept BIOS validation data from a Service Now end customer, the option to configure BIOS data validation is disabled on

the Service Now end customer. For information about disabling BIOS validation on a Service Now end customer, see [“Adding an End Customer to Service Now Configured in Partner Proxy Mode” on page 98](#).

Before you configure BIOS validation, you must accept the BIOS legal notice. The BIOS legal notice is presented to you when you configure BIOS validation for the first time on a Service Now device on a fresh Service Now installation. The BIOS legal notice is also presented when you remove all devices from Service Now and configure BIOS validation after adding the device back to Service Now.

[Figure 24 on page 142](#) and [Figure 25 on page 143](#) show the legal notice displayed on Service Now operating in Partner Proxy and End Customer modes.

Figure 24: BIOS Validation Legal Notice on Service Now Partner

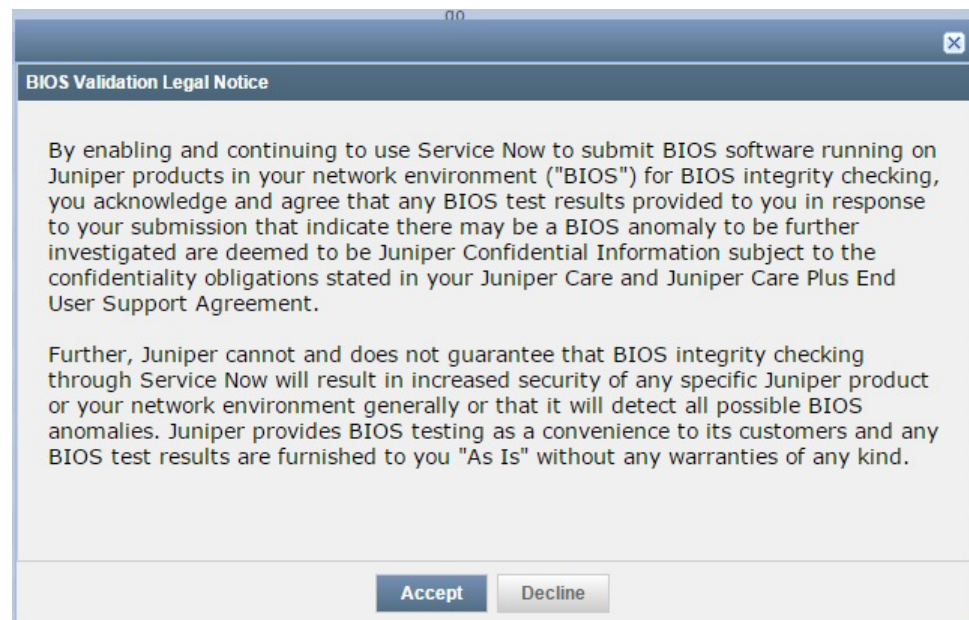
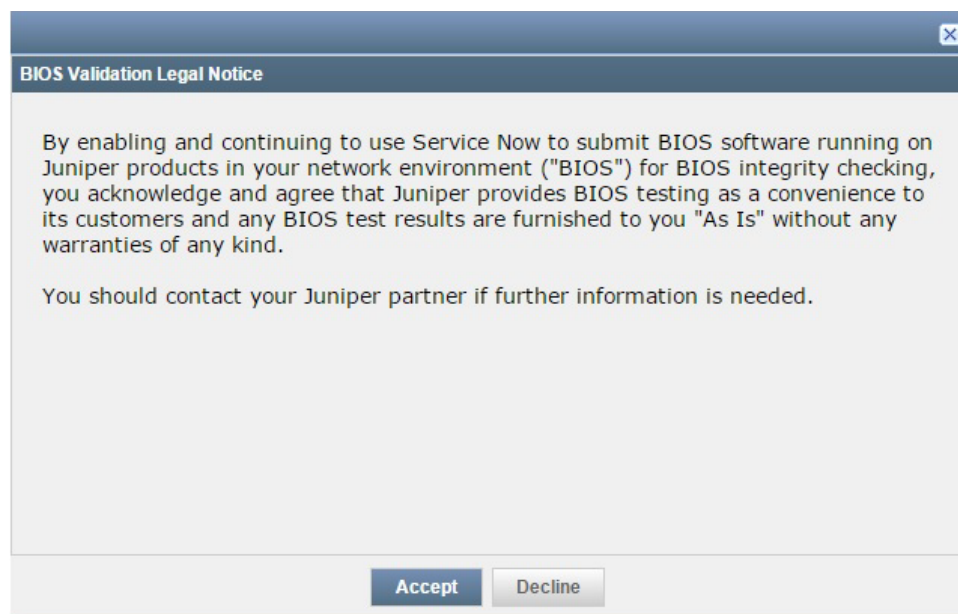


Figure 25: BIOS Validation Legal Notice on Service Now End Customer



On its dashboard, the Device Analysis task displays the status and results of the BIOS validations for all managed devices. Service Now compares the BIOS images received from different devices in a day and submits only the unique BIOS images to JSS for creating BIOS Validation cases; that is, if the same BIOS image is received from thousand managed devices in a day, thousand different incidents are created on Service Now, but only the unique BIOS image is submitted to JSS and one case is created for BIOS validation. If two unique BIOS images are received from managed devices in a day, the two unique images are submitted to JSS and two cases for BIOS validation are created. A maximum of hundred BIOS Health Check cases can be submitted to JSS from an organization in any given day.

To view the status of BIOS validation, on the Service Now navigation tree, select **Service Central > Device Analysis > BIOS Validations**. The BIOS Validations page appears.

[Table 16 on page 143](#) lists the information displayed by the BIOS validations report.

Table 16: BIOS Validations Field Descriptions

Field Name	Description
Incident Details	
Organization	Organization to which the device for which BIOS validation was performed belongs
Device Group	Device group to which the device for which BIOS validation was performed belongs
Connected Member	End customer to which the device belongs if Service Now is operating in Partner Proxy mode
Device	Device for which BIOS validation was performed

Table 16: BIOS Validations Field Descriptions (*continued*)

Field Name	Description
Product	Product family to which the device belongs
Entity	Routing Engine of the device for which BIOS validation was performed
Junos Version	Version of Junos OS installed on the device
Occurred	Date and time when data about BIOS running on the device was collected.
Status	<p>Status of BIOS validation:</p> <ul style="list-style-type: none"> Pending Submission—Service Now has received data for BIOS validation from the device; the data is yet to be submitted to Juniper Support System (JSS). Pending Case Creation—BIOS validation data of the device is received by JSS; JSS is yet to create a case for the received data. Case Created—JSS has created a case for the BIOS validation data received for the device. NOTE: This status is not applicable when Service Now is operating in End Customer mode. Case Creation Failed—JSS failed to create a case for the BIOS validation data received for the device. NOTE: This status is not applicable when Service Now is operating in End Customer mode. Submission Failed—Service Now is unable to submit the BIOS validation data of the device to JSS. Validation Success—Validation of BIOS data by JSS was successful. Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.
Attachment Details	
Attachment	<p>Name of the attachment file</p> <p>You cannot view the contents of the attachment file.</p>
Attachment Size (in byte)	Size of the attachment file in bytes
Command	Command issued on the device to obtain the attachment file
Read Status	Status of reading the attachment from the device
Remarks	Remarks about the attachment.
Log File Details	
Log File	<p>The system log file collected as part of BIOS validation</p> <p>You cannot view the contents of the system log files.</p>
Log File Size (in bytes)	Size of log files in bytes.

Table 16: BIOS Validations Field Descriptions (*continued*)

Field Name	Description
Read Status	Status of reading the log files
Remarks	Remarks about the log files.

From the BIOS Validations page, you can perform the following:

- Delete BIOS validations; see [“Deleting BIOS Validation Results” on page 258](#)
- Export information about BIOS validation results to Excel, see [“Exporting BIOS Validation Results” on page 257](#)

**Related
Documentation**

- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 145](#)
- [Product Health Data Collection Overview on page 147](#)

Configuring BIOS Validation for Verifying BIOS Integrity of a Device

By configuring BIOS validation, you can enable data collection from a device running Junos OS for verifying BIOS integrity of the device. If you are configuring BIOS validation for the first time or after discovering and adding devices to Service Now, you are provided with the BIOS legal notice. You must accept the legal notice before you configure BIOS validation on Service Now devices.

To configure BIOS validation for verifying BIOS integrity:

1. From the Service Now navigation tree, select **Administration > Service Now Devices**.
The Service Now Devices page appears.
2. From the Actions menu, select **Device Analysis > Configure BIOS Validation**.
Alternatively, right-click the device and select **Device Analysis > Configure BIOS Validation**.

The Configure BIOS Validation dialog box appears.



NOTE: The BIOS legal notice appears when you configure BIOS validation for the first time or after you remove and add devices back to Service Now.

Read and accept the legal notice. The Configure BIOS Validation dialog box appears after you accept the legal notice.

Figure 26: Configure BIOS Validation Dialog Box

3. Perform one of the following tasks:
 - If the device is a managed device, under **Currently Managed Device(s)**, select one of the following options:
 - **Do not change setting**—Leaves the settings for collecting data for BIOS validation as is. This option is selected by default.
By default, Service Now is not configured to collect data for BIOS validation.
 - **Do not validate BIOS**—Disables BIOS validation
 - **Validate BIOS**—Enables BIOS validation
 - From the **Apply to** drop-down menu, select one of the following options:
 - **Selected Devices**—Configures BIOS validation on selected devices only
 - **All currently managed devices**—Configures BIOS validation on all devices currently managed by Service Now
 - If the device is a newly discovered device, select one of the following options:
 - **Do not validate BIOS**—Disables BIOS validation
 - **Validate BIOS**—Enables BIOS validation
4. If you select **Validate BIOS**, enter the number of days between successive BIOS validations in the **Interval between BIOS validation (days):** text box.
The number of days between BIOS validations on a device should be between 15 and 30 days. 30 days is the default setting.
5. (Optional) Select the **Schedule BIOS validation on selected device(s) at specified time:** check box to configure the date and time for collecting BIOS data.
6. Click **Submit** to configure BIOS validation or **Cancel** to cancel the configuration.

If you click Submit, a job is created and the Job ID is displayed on the Job Status dialog box.

7. Click the Job ID to view the details and status of the job.

The Success status of the Configure BIOS validation job indicates that a cron job is initiated on the device to collect BIOS data. The cron job is set to execute once a day at 2:00 AM (local time of the device). A BIOS validation record is created on Service Now a few minutes after the cron job is initiated. You can view the BIOS validation record on the job BIOS Validations page (Service Central > Device Analysis > BIOS Validations).

Related Documentation

- [AI-Scripts Overview on page 27](#)
- [BIOS Validation Overview on page 141](#)
- [Exporting BIOS Validation Results on page 257](#)
- [Deleting BIOS Validation Results on page 258](#)

Product Health Data Collection

- [Product Health Data Collection Overview on page 147](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)
- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Enabling Product Health Data Collection on a Device on page 166](#)
- [Aborting a Product Health Data Collection Configuration on page 167](#)
- [Exporting Product Health Data Information to an Excel File on page 168](#)
- [Deleting Product Health Data Files Collected from a Device on page 173](#)
- [Deleting a Product Health Data Collection Configuration from Service Now on page 175](#)

Product Health Data Collection Overview

You use the product health data collection (PHDC) feature of Junos Space Service Now to collect product health data (PHD) from managed devices. PHD is used to assess the health of the devices.

**NOTE:**

- PHDC is not supported on Service Now operating in End Customer mode.
- PHDC is not supported on QFX Series devices in a QFabric.
- PHD can be collected only if AI-Scripts 5.0 or later is installed on a device.
- Within the Service Now application, the product health data collection term, in addition to indicating the feature, indicates individual product health data collection configuration.

PHD comprise the output of various **show** commands of Junos OS, such as **show version**, **show system uptime**, **show chassis fabric summary**, and so on. AI-Scripts installed on managed devices execute the **show** commands and collect the output as a Juniper Message Bundle (JMB). AI-Scripts execute the **show** commands at one-hour interval for the configured number of days. Service Now collects the JMBs and creates a PHD file. The PHD file can be viewed from **Service Central > Device Analysis > Product Health Data Devices** and **Administration > Product Health Data Collection** tasks of the Service Now navigation tree. For information about viewing PHD files, see [“Viewing Product Health Data Files Collected from a Device” on page 149](#).

Figure 27 on page 148 shows the Product Health Data Devices page that lists the devices from which PHD are collected. You can view the status of PHDC on a device on this page. A device is listed on this page when at least one PHD file is collected from it.

Figure 27: Product Health Data Devices Page

Device	Serial Number	Product	View
sn-220-sn1	A05210AA0078	SRX220H	View
sn-650-sn2	AJ4410AA0037	SRX650	View

Table 17 on page 148 describes the fields on the Product Health Data Devices page.

Table 17: Fields on the Product Health Data Devices Page

Field Name	Description
Device	Name of the managed device from which PHD is collected
Serial Number	Serial number of the device
Product	Type of Junos product

Table 17: Fields on the Product Health Data Devices Page (*continued*)

Field Name	Description
View	<p>Link to view the PHD files collected from the device</p> <p>For information about viewing the PHD files, see “Viewing Product Health Data Files Collected from a Device” on page 149.</p>

The collected PHD is submitted to Juniper Support System (JSS) that assesses the health of the device. JSS submits the result of the assessment to the Juniper Networks customer who requested the PHD assessment.

To configure PHDC on Service Now, define the following:

- Devices from which PHD should be collected
- Number of days for which PHD should be collected from the devices
- Whether PHD should be uploaded to JSS
- Whether PHD should be deleted from Service Now after it is uploaded to JSS
- Whether IP addresses should be overwritten with asterisks (*) for security purposes in the PHD files

You can configure PHDC on a device in one of the following ways:

- From the Product Health Data Collection task of the Administration workspace
- From the Service Now Devices task of the Administration workspace

For information about configuring PHDC on managed devices, see [“Configuring Product Health Data Collection on a Device” on page 155](#)

From the Product Health Data page, you can perform the following tasks:

- Export information about devices from which PHD is collected to Excel.
- Export information about the collected PHD files of a device to Excel.

For information about exporting PHD to Excel, see [“Exporting Product Health Data Information to an Excel File” on page 168](#).

**Related
Documentation**

- [Product Health Data Collection Configuration Overview on page 153](#)
- [BIOS Validation Overview on page 141](#)

Viewing Product Health Data Files Collected from a Device

Junos Space Service Now stores product health data (PHD) as PHD files in the Service Now database. From the database, these files are uploaded to Juniper Support System (JSS) for assessment. To view the list of PHD files in the Service Now database, use the View all PHD for this device page, shown in [Figure 28 on page 150](#). You also use this page to download, export, and delete the PHD files.

You can access the View All Product Health Data Files page from the Product Health Data Devices task or the Product Health Data Collection task of the Service Now navigation tree.

Figure 28: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_162001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_162000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

Table 18: Fields on the View All Product Health Data Files Page

Field Name	Description
File Name	<p>Name of the PHD file</p> <p>The name is specified in the following format: <i>hostname-sys_phdc_jmb_ais_health_yyyymmdd_hhmmss</i>, where</p> <ul style="list-style-type: none"> <i>hostname</i> is the hostname of the device from which PHD is collected. <i>yyymmdd</i> is the date when PHD was collected. <i>hhmmss</i> is the time when PHD was collected.
PHDC Name	PHDC configuration used to collect PHD
Received	Date and time when Service Now collected PHD
File Size (Bytes)	Size of the PHD file in bytes
Read Status	<p>Read status of PHD from the device</p> <p>Possible values:</p> <ul style="list-style-type: none"> Not Received—Service Now has not yet collected PHD from the device. Success—Service Now has successfully collected PHD from the device. Failure—Service Now failed to collect PHD from the device. No Longer Available— PHD is no longer available on the device. Successfully Deleted—PHD is successfully deleted from the device after collection by Service Now. Reading from Device—Service Now is currently reading PHD from the device. Read Complete—Service Now has completed reading PHD from the device. Processing—Service Now is processing PHD to create the PHD files.

Table 18: Fields on the View All Product Health Data Files Page (*continued*)

Field Name	Description
Upload Status	Status of uploading PHD files to JSS: <ul style="list-style-type: none">• Not Uploaded—Service Now has not yet uploaded PHD files to JSS.• Success—Service Now has successfully uploaded PHD files to JSS.• Failure—Upload of PHD files to JSS failed.• Uploading—Service Now is uploading PHD files to JSS.
Remarks	Remarks about a failed condition such as failure to read PHD from the device or upload a PHD file to JSS

To view the PHD files collected from a device:

1. • To access the View All Product Health Data Files page from the Product Health Data Devices task:

- a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- b. Click the **View** link of the device for which you want to view PHD files.

The View All Product Health Data Files page appears.

- To access the View All Product Health Data Files page from the Product Health Data Collection task:

- a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- b. Click the link in the Devices field of a PHDC configuration.

The View All Devices of this PHDC page appears as shown in [Figure 29 on page 152](#).

The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 29: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
sn-220-sn1	AG5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
sn-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0

- c. Click the link in the Total Files Available field for the device for which you want to view the PHD files.

The View All Product Health Data Files page appears.

2. On the View All Product Health Data Files page, click one or more files that you want to select for download.

3. Right-click the selection and select **Download Product Health Data File**.

The Download Product Health Data Files dialog box appears.

4. Click the **Download** button.

The Product Health Data Files Download Job Status dialog box appears. The dialog box displays the Download link after the download job is complete.

5. Click the **Download** link.

The dialog box of your browser to open or save the file appears.

- Click the option to open or save the downloaded file.

The product health data file is downloaded as a ***.zip** file.

- Extract the PHD file and view the contents on any text editor such as Notepad or Wordpad.

Related Documentation

- [Product Health Data Collection Overview on page 147](#)
- [Product Health Data Collection Configuration Overview on page 153](#)
- [Exporting Product Health Data Information to an Excel File on page 168](#)
- [Deleting Product Health Data Files Collected from a Device on page 173](#)
- [Deleting a Product Health Data Collection Configuration from Service Now on page 175](#)

Product Health Data Collection Configuration Overview

Service Now provides the Product health data collection (PHDC) feature to collect product health data (PHD) from managed devices for assessment of devices' health. PHD is collected from a device by executing pre-defined Junos OS commands. For information about the Junos OS commands, see

Product health data collection (PHDC) is configured on Service Now by defining the following:

- Devices on which PHD should be collected
- Number of days for which PHD should be collected from the devices
- Whether PHD data should be submitted to Juniper Support System (JSS)
- Whether PHD data should be deleted from Service Now once uploaded to JSS
- Whether IP addresses should be overwritten with asterisks (*) in the PHD files

PHDC configurations on Service Now can be viewed on the Product Health Data Collection page (**Administration > Product Health Data Collection**) as shown in [Figure 30 on page 153](#).

Figure 30: Product Health Data Collection Page

Name	Status	Start Date	End Date	Devices	Domain
M_MX_Group	Running	Jul 27, 2015 11:37:31 PM IST	Aug 26, 2015 11:37:31 PM IST	4	Global
Second Group	Running	Jul 28, 2015 12:54:19 AM IST	Aug 27, 2015 12:54:19 AM IST	4	Global

[Table 19 on page 154](#) lists the fields on the Product Health Data Collection page.

Table 19: Fields on the Product Health Data Collection Page

Field Name	Description
Name	Name of the PHDC configuration
Status	<p>Status of the PHDC configuration</p> <p>Possible values are:</p> <ul style="list-style-type: none"> Scheduled—PHD is scheduled to be collected from all devices assigned to the PHDC configuration at the scheduled time. Starting—PHD collection is starting on all devices included in the PHDC configuration. Running—PHD is being collected from all devices included in the configuration. Failed—PHD collection failed in one or more devices included in the configuration. Stopping—PHD collection is being stopped on one or more devices included in the configuration. Stopped—PHD collection is stopped on one or more devices in included in the configuration. Enabling—PHD collection is enabled on one or more devices in the configuration after being disabled. Disabling—PHD collection is being disabled on one or more devices in the configuration. Aborting—PHD collection is being aborted on all devices of the configuration.
Start Date	Date and time PHD collection is scheduled to start or PHD collection started
End Date	Date and time to end PHD collection or PHD collection ended (if the PHDC status is completed)
Devices	<p>Number of devices to which the PHDC configuration is assigned</p> <p>Click the link to view the details of devices, the status of PHD collection on the devices and view the PHD files collected from individual devices.</p> <p>See “Product Health Data Collection Overview” on page 147 for details on the status of PHD collection on a device.</p>
Domain	<p>Domain to which the PHDC configuration is assigned</p> <p>By default, a PHDC configuration is assigned to the domain in which the user creating the PHDC configuration is logged in.</p>

Associated Actions

On the Product Health Data Collection page, you can perform the following actions:

- Modify a PHDC configuration; see [“Modifying a Product Health Data Collection Configuration”](#) on page 160 for details.
- Reschedule a PHDC configuration; see [“Rescheduling a Product Health Data Collection Configuration”](#) on page 163 for details.
- Retry collecting PHD from devices on which an earlier attempt to collect PHD failed; see [“Retrying Collecting Product Health Data from a Device”](#) on page 164 for details.

- Enable PHD collection on devices; see [“Enabling Product Health Data Collection on a Device” on page 166](#) for details.
- Disable PHD collection on devices; see [“Disabling Product Health Data Collection on a Device” on page 165](#) for details.
- Abort PHD collection on devices; see [“Aborting a Product Health Data Collection Configuration” on page 167](#) for details.
- Delete a PHDC configuration; see [“Deleting a Product Health Data Collection Configuration from Service Now” on page 175](#) for details.
- Assign a PHDC configuration to another domain; see [“Assigning a Service Now Object to a Domain” on page 50](#) for details.

**Related
Documentation**

- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Product Health Data Collection Overview on page 147](#)

Configuring Product Health Data Collection on a Device

Product health data collection (PHDC) configurations are listed on the Product Health Data Collection page of the Administration workspace.

Junos Space Service Now provides the following ways to configure PHDC on managed devices:

- [Configuring PHDC by Using the Product Health Data Collection Task on page 155](#)
- [Configuring PHDC by Using the Service Now Devices Task on page 157](#)

Configuring PHDC by Using the Product Health Data Collection Task

Configuring PHDC from Product Health Data Collection task involves selecting devices on which to configure PHDC and then configuring the parameters.



NOTE: PHDC consumes CPU cycles and disk resources of the device. Therefore, performance of the device might be affected while PHD is being collected.

To configure PHDC on a device from the Product Health Data Collection task:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection > Configure PHDC**.

The Configure PHDC page appears as shown in [Figure 31 on page 156](#).

Figure 31: Create PHDC Page

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
<input type="checkbox"/> Test-Org	Device Group for Test-Org	sn-3600-sn1	AB3510AA0021	SRX3600	12.1X44-D40.2	5.0/20150722_2005_barnstrong
<input type="checkbox"/> Test-Org	Device Group for Test-Org	sn-3600-sn2	AB3510AA0022	SRX3600	12.1X44-D40.2	5.0/20150722_2005_barnstrong
<input type="checkbox"/> Test-Org	Device Group for Test-Org	compion	JN1207242AJA	PTX5000	14.2R3	5.0/20150722_2005_barnstrong
<input type="checkbox"/> Test-Org	Device Group for Test-Org	r14mx960wf	JN1218FCCAFA	MX960	14.1-20150717.0	5.0/20150722_2005_barnstrong

2. Enter a name for the PHDC configuration.

The name of a PHDC configuration must have 4 to 64 alphanumeric characters. Underscore (_) and hyphen (-) are the only special characters are allowed.

3. Click on the devices that you want to include in the PHDC configuration. Alternatively, select the check box next to the **Organization** field to include all devices listed in the PHDC configuration.
4. Click **Next**.

The Configure Product Health Data Collection page appears as shown in [Figure 32 on page 156](#).

Figure 32: Configure Product Health Data Collection

Collection Period (days): 30

☒ Upload Product Health Data files to Juniper

☒ Delete Product Health Data files after upload

☒ Mask IP addresses before uploading Product Health Data files

Note: Product Health Data Collection requires CPU and disk resources on the Junos device and therefore might impact device performance.

☒ Schedule Product Health Data Collection at specified time

Date and time: 08/07/15 4:31 PM IST

Back Submit Cancel

5. On the Configure Product Health Data Collection page, configure options as follows:

- **Collection Period (days):** Enter the number of days for product health data (PHD) should be collected from the devices.

Number of days can range from 1 to 90. The default value is 30 days.

- **Upload Product Health Data files to Juniper:** Select this check box to upload PHD files collected from devices to Juniper Support System (JSS).

This option is selected by default.



NOTE: If you clear this check box, PHD files are not uploaded to JSS. If required later, you cannot upload PHD files to JSS.

- **Delete Product Health Data files after upload:** Select this check box to delete PHD files from Service Now immediately after they are uploaded to JSS.

This option is selected by default.



NOTE: If you clear this check box, PHD files are automatically deleted four days after the files are collected by Service Now.

- **Mask IP addresses before uploading Product Health Data files:** Select this check box to replace IP addresses with asterisks (*) in collected PHD.

This option is selected by default.

- (Optional) **Schedule PHD Collection at specified time:** Select this check box to schedule a date and time for collecting PHD.

6. Click **Submit** to submit the PHDC configuration.

The PHDC configuration is listed on the Product Health Data Collection page.

If a date and time is not scheduled for PHD collection, PHD collection is started immediately on devices included in the configuration.

Configuring PHDC by Using the Service Now Devices Task

Junos Space Service Now allows you to configure PHD on a managed device from the Service Now Devices task after you assign the device to a product health data collection (PHDC) configuration. You can add the device to a PHDC configuration by creating a new configuration or to an existing PHDC configuration. A device can be added to an existing PHDC configuration only if the configuration is in the Scheduled or Running state. Once assigned to a PHDC configuration in Scheduled or Running state, a device cannot be assigned to any other PHDC configuration.



NOTE: PHDC consumes CPU cycles and disk resources of a device. Therefore performance might be affected while PHD is collected from the device.

To configure PHD collection on a device:

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

The Service Now Devices page appears.

2. Select one or more devices to configure PHDC.



NOTE: PHDC can be configured on a maximum of 500 devices at a time.

3. From the Actions menu, select **Device Analysis > Configure Product Health Data Collection**. Alternatively, right-click the selected devices and select **Device Analysis > Configure Product Health Data Collection**.

The Configure Product Health Data Collection dialog box appears as show in [Figure 33 on page 158](#).

Figure 33: Configure Product Health Data Collection Dialog Box

Configure Product Health Data Collection

Prodcut Health Data

☐ Add to an existing PHDC ☒ Create a new PHDC

Select Devices

Apply to: Selected device(s)

Configure Product Health Data Collection

Name:

Collection Period (days):

☒ Upload Product Health Data Collection files to Juniper

☒ Delete Product Health Data Collection files after upload

☒ Mask IP addresses before uploading Product Health Data files

Note: Product Health Data Collection requires CPU and disk resources on the Junos device and therefore might impact device performance.

☒ **Schedule Product Health Data Collection at specified time**

Date and time: IST

Submit **Cancel**

4. On the Configure Product Health Data Collection dialog box, do one of the following:
 - Add the selected devices to an existing PHDC configuration.

To add the selected devices to an existing PHDC configuration:

- a. Click **Add to an existing PHDC**.
 - b. Select a PHDC configuration from the **PHDC** drop-down list to add the device.
- Add the selected devices to a new PHDC configuration.

To add the selected devices to a new PHDC configuration:

- a. Click **Create a new PHDC**.
- b. From the **Apply to** drop-down list, select one of the following:
 - **Selected device(s)** to configure PHD collection on all devices selected on the Service Now Devices page
 - **All devices in the current domain** to configure PHD collection on all managed devices in the domain in which you are logged in
 - **Select Tag** to configure PHD collection on devices having a specific tag

The Select from available Tags drop-down list appears when you select the Select tag option. Select a tag from the **Select from available Tags** drop-down list.

- **Select Device Group** to configure PHD collection on devices belonging to a specific device group

The Select from available Device Groups drop-down list appears when you select the Select Device Group option. Select a device group from the **Select from available Device Groups** drop-down list.

- c. Under Configure PHDC, configure options as follows:
 - **Name:** Enter a name for the PHDC configuration. The name of a PHDC configuration must have 4 to 64 alphanumeric characters. Underscore(_) and hyphen (-) are the only special characters allowed.
 - **Collection Period (days):** Enter the number of days for collecting product health data (PHD) from the devices.

Number of days can range from 1 to 90. The default value is 30 days.

- **Upload Product Health Data files to Juniper:** Select this check box to upload PHD files collected from devices to Juniper Support System (JSS).

This option is selected by default.



NOTE: If you clear this check box, PHD files are not uploaded to JSS. If required later, you cannot upload PHD files to JSS.

- **Delete Product Health Data files after upload:** Select this check box to delete PHD files from Service Now immediately after they are uploaded to JSS.

This option is selected by default.



NOTE: If you clear this check box, PHD files are automatically deleted four days after the files are collected by Service Now.

- **Mask IP addresses before uploading Product Health Data files:** Select this check box to replace IP addresses with asterisks (*) in the collected PHD.

This option is selected by default.

- **(Optional) Schedule PHD Collection at specified time:** Select this check box to schedule a date and time for collecting PHD from the selected devices.

5. Click **Submit** to submit the PHDC configuration on the device.

The PHDC configuration is saved on Service Now and can be viewed on the Product Health Data Collection page (**Administration > Product Health Data Collection**).

If a time is scheduled, the PHD collection is initiated on the device at the scheduled time. If a time is not scheduled, PHD collection is started immediately.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Enabling Product Health Data Collection on a Device on page 166](#)
- [Aborting a Product Health Data Collection Configuration on page 167](#)
- [Exporting Product Health Data Information to an Excel File on page 168](#)

Modifying a Product Health Data Collection Configuration

The parameters of a PHDC configuration that can be modified depend on the state of the PHDC configuration. You cannot modify the name of a PHDC configuration.

You can modify the following parameters of a PHDC configuration:

- Devices assigned to PHDC

Devices can be assigned and deleted from a PHDC configuration if the PHDC configuration status is not Aborted.

When you assign a device to a PHDC configuration in the Running state, product health data (PHD) is collected from the device for the number of days that are remaining in the configuration. For example, if you assign a device to a PHDC configuration that is in running state and configured to run for 10 days on the fourth day of PHD collection, PHD is collected from the device for the remaining six days.

- Collection period

PHD collection period can be changed if the PHDC configuration status is not Aborted.

To extend the number of days of PHD collection, the number of days to be extended should be added to the collection period currently configured. For example, to extend PHD collection period of 30 days by ten days, enter 40 (30 + 10) for the Collection period.

To reduce the number of days of PHD collection, the number of days to be reduced should be removed from the collection period currently configured. For example, to reduce the collection period by 10 days, enter 20 (30 - 10) as the Collection period. If you are modifying the collection period 20 days after the PHD collection started (say on the 22nd day or 23rd day, the PHD collection is stopped on the devices.

- Upload Product Health Data Files to Juniper

The option to upload PHD files to JSS can be changed only when the status of a PHDC configuration is Scheduled.

- Delete PHD files after upload

The option to delete PHD files from Service Now after upload to JSS can be changed only when the status of a PHDC configuration is Scheduled.

- Mask IP address before uploading PHD files

The option to mask IP address in the PHD files before uploading the files to JSS can be changed only when the status of a PHDC configuration is Scheduled.

To modify a PHDC configuration:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.
- The Product Health Data Collection page appears.
2. On the Product Health Data Collection page, select the PHDC configuration that you want to modify.
 3. From the Actions menu, select **Modify Product Health Data Collection group**. Alternatively, right-click the PHDC configuration and select **Modify Product Health Data Collection**.

The Modify Product Health Data Collection page appears as shown in figure.

Figure 34: Modify Product Health Data Collection Page

The screenshot displays the 'Modify Product Health Data Collection' page. The left sidebar contains the navigation tree with 'Product Health Data Collection' selected. The main content area has a header 'Choose devices to include in the Product Health Data Collection' and a text input field 'Name: M_MX_Group'. Below this is a table with the following data:

<input checked="" type="checkbox"/>	Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
<input checked="" type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m10i-sys	K1915	M10i	11.4R7.5	5.0/20150722_0138
<input checked="" type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx320-sys	F7760	M320	12.3R8.7	5.0/20150722_0138
<input checked="" type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx240-sys	JN121EB69AFC	MX240	12.3R8.7	5.0/20150722_0138
<input checked="" type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	mx-480-sn2	JN11742FFAFB	MX480	12.3R6.6	5.0/20150722_0138

4. (Optional) Click the **Show Selected Devices** link to view the devices included in the PHDC configuration.
5. Add or remove devices from the PHDC configuration by selecting or clearing the check boxes provided next to the devices.
6. Click **Next**.

The Modify Product Health Data Collection parameters are displayed.

Figure 35: Modify Product Health Data Collection Parameters

Modify Product Health Data Collection

Collection Start date: Aug 6, 2015 11:57:46 AM IST

Collection Period (days): 30

☒ Upload Product Health Data files to Juniper

☐ Delete Product Health Data files after upload

☐ Mask IP addresses before uploading Product Health Data files

Note: Product Health Data Collection requires CPU and disk resources on the Junos device and therefore might impact device performance.

Back Submit Cancel

7. Modify **Collection Period (days)**.

The PHD Collection Period can vary from 1 to 90 days.

8. If the PHDC configuration is in Scheduled state, you can modify the following parameters:

- Upload Product Health Data files to Juniper
- Delete Product Health Data files after upload
- Mask IP addresses before uploading Product Health Data files

9. Click **Submit**.

A message indicating the successful modification of the PHDC configuration is displayed.

Related Documentation

- [Aborting a Product Health Data Collection Configuration on page 167](#)
- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)

- [Viewing Product Health Data Files Collected from a Device on page 149](#)
- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)

Rescheduling a Product Health Data Collection Configuration

You can reschedule a product health data collection (PHDC) configuration if the PHDC status of the configuration is Completed. See “[Product Health Data Collection Configuration Overview](#)” on page 153 for details on the status of PHDC configuration.

When you reschedule a PHDC configuration, **Copy of** prefix is added to the name of the PHDC configuration. While rescheduling, you can add or remove devices from the configuration and modify the PHD collection period.

To reschedule a PHDC configuration:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.
The Product Health Data Collection page appears.
2. On the Product Health Data Collection page, select the PHDC configuration that you want to reschedule.
3. From the Actions menu, select **Reschedule**. Alternatively, right-click the PHDC configuration and select **Reschedule**.
The Reschedule page appears.
4. (Optional) Select or remove devices from the PHDC configuration by selecting or clearing the check boxes provided next to the devices.
5. Click **Next**.
The Configure Product Health Data Collection parameters appear.
6. (Optional) Modify the **Collection Period (days)**.
7. (Optional) Select a schedule date and time to start the PHD collection.
8. Click **Submit** to reschedule PHDC or click **Cancel** to cancel rescheduling PHDC.

Clicking Submit displays a message indicating the successful rescheduling of PHDC configuration. If a date and time is not scheduled for PHD collection, PHD collection is started immediately and the status of the PHDC configuration is changed to starting and then running.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Aborting a Product Health Data Collection Configuration on page 167](#)
- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)

- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)

Retrying Collecting Product Health Data from a Device

You can retry collecting product health data (PHD) on a device assigned to a product health data collection (PHDC) configuration if an earlier attempt to collect PHD from the device failed (that is, the PHD collection status of the device is Failed) and if the status of PHDC configuration is Running. See [“Product Health Data Collection Overview” on page 147](#) for details about the statuses of PHD collection on a device and [“Product Health Data Collection Configuration Overview” on page 153](#) for details about the statuses of PHDC configuration.

To retry collecting PHD from a device on which PHD collection failed:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.
- The Product Health Data Collection page appears.
2. On the Product Health Data Collection page, select the PHDC configuration assigned to the device on which you want to retry collecting PHD.
3. From the Actions menu, select **Retry on failed devices**. Alternatively, right-click the PHDC configuration and select **Retry on failed devices**.

The Retry on failed devices page appears as shown in [Figure 36 on page 164](#). The page lists the devices of the configuration on which an earlier attempt to collect PHD failed.

Figure 36: Retry on Failed Devices Page

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m10i-sys	K1915	M10i	11.4R7.5	
PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx320-sys	F7760	M320	12.3R8.7	
PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx240-sys	JN121EB69AFC	MX240	12.3R8.7	
PHD-Test-ORG	Default for PHD-Test-ORG	mx-480-sn2	JN11742FFAFB	MX480	12.3R6.6	

4. In the table, click the devices on which you want to retry PHD collection.
5. Click **Submit** to retry PHD collection or click **Cancel** to cancel retrying PHD collection.

Clicking Submit displays a message indicating PHD collection is attempted again on selected devices. The PHD collection status for the devices is changed to Scheduled, Starting and then Running if the retry is successful.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Aborting a Product Health Data Collection Configuration on page 167](#)

- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)

Disabling Product Health Data Collection on a Device

Product health data (PHD) collection can be disabled on any device assigned to a PHDC configuration if the PHD collection status of the device is Running or Enabled and the status of the PHDC configuration is Running. This option allows you to disable PHD collection selectively on devices in a PHDC configuration without affecting the PHD collection on other devices.

To disable PHD collection on a device of a PHDC configuration:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, click the PHDC configuration to which the device on which you want to disable PHD collection is assigned.
3. From the Actions menu, select **Disable Collection on devices**. Alternatively, right-click the PHDC configuration and select **Disable Collection on devices**.

The Disable Collection on devices page appears as shown in [Figure 37 on page 165](#).

The page lists the devices on which PHD collection can be disabled.

Figure 37: Disable Collection on Devices Page

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
<input checked="" type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m10i-sys	M10i	11.4R7.5	
<input type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m320-sys	M320	12.3R8.7	
<input type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx240-sys	JN121EB69AFC	12.3R8.7	
<input type="checkbox"/>	PHD-Test-ORG	Default for PHD-Test-ORG	mx-480-sn2	JN11742FFAFB	MX480	12.3R8.6

4. In the table, click the devices on which you want to disable PHD collection.
5. Click **Submit** to disable PHD collection on selected devices or click **Cancel** to cancel disabling PHD collection.

Clicking Submit displays a message indicating PHD collection is disabled on selected devices and the PHD collection status for the devices is changed to disabled.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)

- [Aborting a Product Health Data Collection Configuration on page 167](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)

Enabling Product Health Data Collection on a Device

Product health data (PHD) collection can be enabled on devices of a PHDC configuration if PHD collection was earlier disabled on the devices. This option allows you to enable PHD collection selectively on a device in a PHDC configuration without affecting the disabled status of PHD collection on other devices.

To enable PHD collection on a device of a PHDC configuration:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, click the PHDC configuration to which the device on which you want to enable PHD collection is assigned.
3. From the Actions menu, select **Enable Collection on devices**. Alternatively, right-click the PHDC configuration and select **Enable Collection on devices**.

The Enable Collection on Devices page appears as shown in [Figure 38 on page 166](#). The page lists the devices on which PHDC can be enabled.

Figure 38: Enable Collection on Devices Page

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
<input type="checkbox"/> PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m10i-sys	K1915	M10I	11.4R7.5	
<input type="checkbox"/> PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx320-sys	F7760	M320	12.3R8.7	

4. In the table, click the devices on which you want to enable PHD collection.
5. (Optional) Click the **Show Selected Devices** link to view the devices selected for enabling PHDC.

Click **Close** to return back to the Enable Collection on Devices page.

6. Click **Submit** to enable PHD collection on selected devices or click **Cancel** to cancel enabling PHD collection.

Clicking Submit displays a message indicating PHD collection is enabled on selected devices and the PHD collection status for the device is changed to enabled.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Aborting a Product Health Data Collection Configuration on page 167](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)

Aborting a Product Health Data Collection Configuration

You can abort product health data collection (PHDC) configuration when the status of PHDC is Running. This action aborts PHD collection on all devices assigned to the PHDC configuration.



NOTE: Once you abort a PHDC configuration, you can only delete the configuration. You cannot move it to any other state.

To abort PHDC configuration:

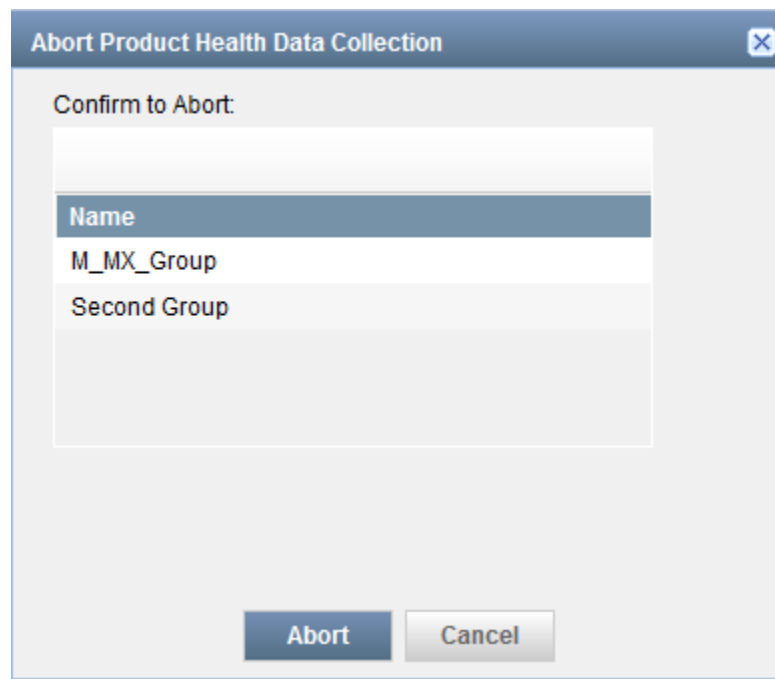
1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select one or more PHDC configurations that you want to abort.
3. From the Actions menu, select **Abort**. Alternatively, right-click the PHDC configuration and select **Abort**.

The Abort Product Health Data Collection dialog box is displayed as shown in [Figure 39 on page 168](#).

Figure 39: Abort Product Health Data Collection Dialog Box



4. Click **Abort** to abort the PHDC configuration or click **Cancel** to cancel aborting.

Clicking Submit displays a message indicating the PHDC configuration is successfully aborted. The status of the PHDC configuration and the PHD collection status of the devices are set to aborted.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Enabling Product Health Data Collection on a Device on page 166](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)

Exporting Product Health Data Information to an Excel File

Junos Space Service Now provides the Export and Export All options on the Product Health Data Devices task to export the following information in an Excel file:

- Devices on which product health data collection (PHDC) is configured

The exported Excel file is named in the format **PHDDevices_YYYY-MM-DD_hhmmss**, where *YYYY-MM-DD* and *hhmmss* are the date and time the Excel file is created.

Figure 40 on page 169 shows a sample of the information about devices exported to Excel.

Figure 40: PHDC Information of Devices Exported to Excel

	A	B	C	D	E	F	G	H
1								
2	Device	Serial Number	PHD Group Name	Start Date	Status	Total Files Received	Last Uploaded	Status Message
3	mx-80-sn2	D4358	Test-group	2015-07-16 01:32:51.36	Running	28		
4	mx-480-sn1	JN11AFF42AFB	Test-group	2015-07-16 01:32:51.36	Running	28		
5								
6								

- Product health data (PHD) files collected from individual devices

The exported Excel file is named in the format

PHDInfoReport-*hostname*_*yyy-mm-dd_hhmmss*, where *hostname* is the hostname of the device from which the PHD files were collected and *yyy-mm-dd* and *hhmmss* are the date and time the Excel file is created.

Figure 41 on page 169 shows a sample of the information about PHD files exported to Excel.

Figure 41: PHD Files Information Exported to Excel

	A	B	C	D	E	F	G
1							
2	Device Name	mx-480-sn1					
3	Total Number of PHD	25					
4							
5	File Name	Group Name	Size (Bytes)	Received (UTC)	Read Status	Upload Status	Remarks
6							
7	mx-480-sn1_phdc_jmb	Test-group	59548	2015-07-16 10:18:08.15	Success	Success	
8	mx-480-sn1_phdc_jmb	Test-group	59984	2015-07-16 23:18:06.51	Success	Not Uploaded	
9	mx-480-sn1_phdc_jmb	Test-group	N/A	2015-07-17 02:19:22.55	Not Received	Not Uploaded	
10	mx-480-sn1_phdc_jmb	Test-group	59561	2015-07-16 13:18:03.25	Success	Success	
11	mx-480-sn1_phdc_jmb	Test-group	90203	2015-07-16 02:19:16.46	Success	Success	
12	mx-480-sn1_phdc_jmb	Test-group	59552	2015-07-16 05:18:07.90	Success	Success	
13	mx-480-sn1_phdc_jmb	Test-group	59758	2015-07-16 16:18:03.51	Success	Success	
14	mx-480-sn1_phdc_jmb	Test-group	59561	2015-07-16 19:18:08.45	Success	Not Uploaded	
15	mx-480-sn1_phdc_jmb	Test-group	59416	2015-07-16 06:18:01.12	Success	Success	
16	mx-480-sn1_phdc_jmb	Test-group	59832	2015-07-16 22:18:06.82	Success	Not Uploaded	
17	mx-480-sn1_phdc_jmb	Test-group	59812	2015-07-16 09:18:03.65	Success	Success	
18	mx-480-sn1_phdc_jmb	Test-group	59569	2015-07-17 01:18:07.51	Success	Not Uploaded	
19	mx-480-sn1_phdc_jmb	Test-group	59556	2015-07-16 12:18:03.25	Success	Success	
20	mx-480-sn1_phdc_jmb	Test-group	59563	2015-07-16 15:18:10.06	Success	Success	
21	mx-480-sn1_phdc_jmb	Test-group	59949	2015-07-16 03:18:01.24	Success	Success	

To export PHDC data in Excel format, see the following:

- Exporting Information about Devices on which PHDC is configured on page 169
- Exporting Data about PHD Files Collected from a Device on page 171

Exporting Information about Devices on which PHDC is configured

You can export Information about devices on which PHDC is configured from the Product Health Data Devices task or the Product Health Data Collection task of the Service Now navigation tree. When you export information about devices from the Product Health Data Devices task in Service Central workspace, information about all the managed devices in Service Now from which PHD is collected is exported; whereas, when you export information about devices from the Product Health Data Collection task in the Administration workspace, information about devices in a specific PHDC configuration is exported.

To export information about devices on which PHDC is configured to Excel:

1. • To export the information from the Product Health Data Devices task:
 - a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- To export the PHD files from the Product Health Data Collection task:
 - a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- b. Click the link on the Devices column of a PHDC configuration.

The View all Devices of this PHDC page appears as shown in [Figure 42 on page 170](#). The View all Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 42: View all Devices of this PHDC

Device	Serial Number	Product	Start Date	Status	Total Files Available
snx-220-sn1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snx-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0

2. • To export information about all the devices, right-click on a row and select **Export All**.

The Export All Product Health Data Devices dialog box is displayed. The dialog box displays the **Export All Product Health Data Devices to Excel** link to download the Excel file.

- To export information about selected devices, select the devices and then right-click and select **Export Selected**.

The Export Selected Product Health Data Devices dialog box is displayed. The dialog box displays the **Export selected Product Health Data Devices to Excel** link to download the Excel file.

3. Click the **Export selected Product Health Data Devices to Excel** or **Export All Product Health Data Devices to Excel** link displayed on the dialog box.

The dialog box of your browser to open or save a file appears.

4. Choose the option to open or save the Excel file.

Exporting Data about PHD Files Collected from a Device

You can export the PHD files from the Product Health Data Devices task in the Service Central workspace or the Product Health Data Collection task in the Administration workspace of the Service Now navigation tree.

To export data about PHD files collected from a device:

1. • To export the PHD files from the Product Health Data Devices task:
 - a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- b. Click the **View** link of the device for which you want to export PHD files.

The View All Product Health Data Files page appears as shown in [Figure 43 on page 172](#).

Figure 43: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

- To export the PHD files from the Product Health Data Collection task:
 - a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- b. Click the link in the Devices column of a PHDC configuration.

The View All Devices of this PHDC page appears as shown in [Figure 44 on page 172](#).

The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 44: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
snx-220-sn1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snx-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0

- c. Click the link in the Total Files Available column for the device for which you want to export the PHD files.

The View all Product Health Data Files page appears.

2. • To export information about all the PHD files collected for the device, right-click a row on the page and select **Export All**.

The Export All Product Health Data Information dialog box is displayed. The dialog box contains the **Export all Product Health Data files information to Excel** link to download the Excel file.

- To export information about selected PHD files, select the files to be exported and then right-click and select **Export**.

The Export Selected Product Health Data Information dialog box is displayed. The dialog box contains the **Export selected Product Health Data files information to Excel** link to download the Excel file.

3. Click the **Export selected Product Health Data files information to Excel** or **Export all Product Health Data files information to Excel** link displayed on the dialog box.

The dialog box of your browser to open or save a file appears.

4. Choose the option to open or save the Excel file.

Related Documentation

- [Product Health Data Collection Overview on page 147](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)
- [Product Health Data Collection Configuration Overview on page 153](#)

Deleting Product Health Data Files Collected from a Device

The product health data (PHD) files collected from managed devices are stored in Junos Space Service Now database and uploaded to Juniper Support System (JSS) for assessing the health of the device. If configured to be deleted, the PHD files are deleted immediately after they are uploaded to JSS. Otherwise, the PHD files are deleted from the Service Now database four days after they are created.

Service Now provides the delete option to delete the PHD files if you want to delete the PHD files. You can delete the PHD files from the Product Health Data Devices task in the Service Central workspace or the Product Health Data Collection task in the Administration workspace of the Service Now navigation tree.

To delete the PHD files collected from a device:

1. • To delete the PHD files from the Product Health Data Devices task of the Service Central workspace:
 - a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- b. Click the **View** link of the device for which you want to delete PHD files.

The View All Product Health Data Files page appears as shown in [Figure 45 on page 174](#).

Figure 45: View All Product Health Data Files Page

Service Central > Device Analysis > Product Health Data Devices > View all Product Health Data Files						
Service Now	Back					
Dashboard	File Name	PHDC Name	Received ~	File Size (Bytes)	Read Status	Upload Status
Service Central	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21450	Success	Uploaded
Incidents	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
View Tech Support Cases	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
Information	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
Device Analysis	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
BIOS Validations	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
Product Health Data Device	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
JMB Errors	ex-4200-sr1_phdc_jmb_ais_health_2015_0416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded
Notifications						
Devices						
Jobs						
Administration						
Organizations						
Device Groups						
Service Now Devices						
Event Profiles						
Global Settings						
Auto Submit Policy						
Product Health Data Collector						
Address Group						
Email Templates						

- To delete the PHD files from the Product Health Data Collection task of the Administration workspace:
 - From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- Click the link in the Devices field of a PHDC configuration.

The View All Devices of this PHDC page appears as shown in [Figure 46 on page 174](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 46: View All Devices of this PHDC Page

Administration > Product Health Data Collection > View all Devices of this PHDC						
Service Now	Back					
Device	Serial Number	Product	Start Date	Status	Total Files Available	
snx-220-sn1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0	
snx-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0	

- Click the link in the Total Files Available field for the device for which you want to delete the PHD files.

The View All Product Health Data Files page appears.

2. On the View All Product Health Data Files:

- To delete selected PHD files, select the files that you want to delete and then select **Delete Product Health Data**.

The Delete Selected Product Health Data Files dialog box appears.

- To delete all the PHD files collected from the device, right-click any row and select **Delete All Product Health Data**.

The Delete All Product Health Data Files dialog box appears.

3. Click the **Delete** button to delete or the **Cancel** button to cancel the deletion.

If you click the Delete button, a message indicating that the files are deleted is displayed.

**Related
Documentation**

- [Product Health Data Collection Overview on page 147](#)
- [Product Health Data Collection Configuration Overview on page 153](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)
- [Exporting Product Health Data Information to an Excel File on page 168](#)

Deleting a Product Health Data Collection Configuration from Service Now

A product health data collection (PHDC) configuration can be deleted from Junos Space Service Now if the status of the configuration is not Running.

To delete a PHDC configuration:

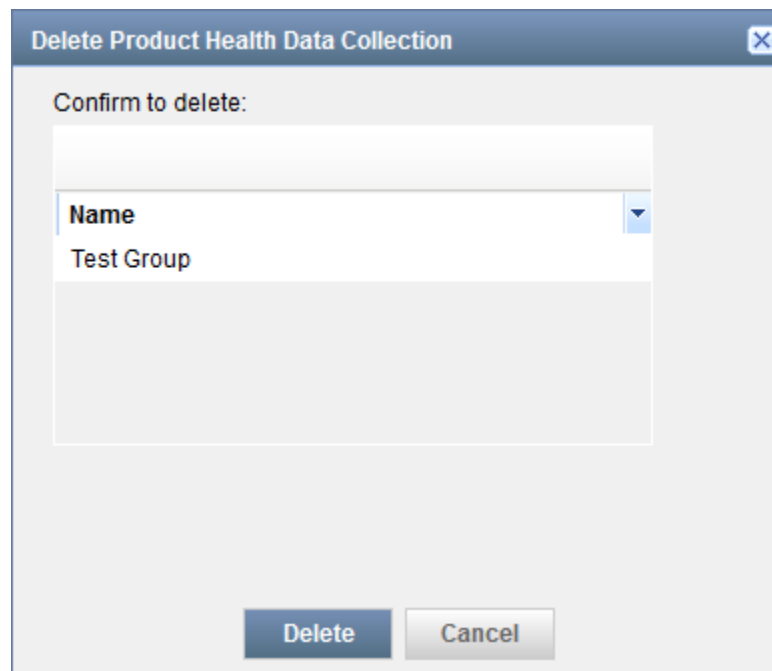
1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select the PHDC configuration that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, right-click the PHDC configuration and select **Delete**.

The Delete Product Health Data Collection dialog box appears as shown in [Figure 47 on page 176](#).

Figure 47: View all Product Health Data Files Page



4. Click **Delete** to delete the PHDC configuration or click **Cancel** to cancel the deletion.

Clicking Submit displays a message indicating the PHDC configuration is successfully deleted.

Related Documentation

- [Product Health Data Collection Configuration Overview on page 153](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)
- [Viewing Product Health Data Files Collected from a Device on page 149](#)
- [Disabling Product Health Data Collection on a Device on page 165](#)
- [Enabling Product Health Data Collection on a Device on page 166](#)
- [Retrying Collecting Product Health Data from a Device on page 164](#)
- [Rescheduling a Product Health Data Collection Configuration on page 163](#)
- [Modifying a Product Health Data Collection Configuration on page 160](#)

Event Profiles and AI-Scripts

- [Event Profiles Overview on page 177](#)
- [Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview on page 182](#)
- [Adding an Event Profile to Junos Space Service Now on page 185](#)
- [Cloning an Event Profile on page 189](#)
- [Importing Event Profiles into Junos Space Service Now in XML Format on page 191](#)

- [Exporting Event Profiles from Junos Space Service Now in XML Format on page 192](#)
- [Deleting Event Profiles from Junos Space Service Now on page 194](#)
- [Viewing an Event Profile on page 195](#)
- [Pushing an Event Profile to Devices on page 195](#)
- [Displaying Devices Associated with an Event Profile on page 198](#)
- [Setting an Event Profile as the Default Event Profile in Junos Space Service Now on page 198](#)
- [Exporting Events Data in Excel Format on page 199](#)
- [Adding a Script Bundle to Junos Space Service Now on page 200](#)
- [Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now on page 200](#)
- [Deleting a Script Bundle from Junos Space Service Now on page 201](#)

Event Profiles Overview

An event profile is a set of event scripts, selected from an AI-Scripts bundle that you install on Service Now devices. The event scripts in the event profile determine the events for which an event Juniper Message Bundle (JMB) JMB is generated on the device.

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 Junos Space Service Now” on page 200](#)).

Service Now also has a default event profile that is associated with the default AI-Scripts bundle. For new Service Now installations 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 48 on page 178). 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 48 on page 178, Base_Profile_3_7R1_2 is the default event profile. a

Figure 48: 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

Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview

Advanced Insight Scripts (AI-Scripts) provide the intelligence that managed devices need to automatically detect and report hardware and software failure or other functional abnormalities. For AI-Scripts to provide intelligence to a device, AI-Scripts must be installed and AI-Scripts configuration committed on a device running Junos OS.

From Service Now release 15.1R1 and AI-Scripts Release 5.0R1, Service Now pushes and commits a static AI-Scripts configuration when AI-Scripts Release 5.0R1 is installed (or an earlier version is upgraded to Release 5.0R1) on the device for the first time. The static configuration, once committed on the device is used during successive installation or upgrade of AI-Scripts, thereby, eliminating the need for pushing and committing AI-Scripts configuration for each AI-Scripts installation or upgrade.

The Static AI-Scripts comprises the following Junos OS commands:

```
set groups juniper-ais system scripts op file ais_change_perm.slax
set groups juniper-ais system scripts op file ais_core_perm.slax
set groups juniper-ais system scripts op file on-demand.slax
set groups juniper-ais system scripts op file remove-jais.slax
set groups juniper-ais system scripts op file ais_arc.slax
set groups juniper-ais system scripts op file ais-attach-file.slax
set groups juniper-ais system scripts op file stop-ais-now.slax
set groups juniper-ais system scripts op file ais_signalSN.slax
set groups juniper-ais system scripts op file ais_core_chm.slax
set groups juniper-ais system scripts op file ais_all_chm.slax
set groups juniper-ais system scripts op file att_signalSN.slax
set groups juniper-ais system scripts op file ais-rsi-chk.slax
set groups juniper-ais system scripts op file ais-param-set.slax
set groups juniper-ais system scripts op file ais-sleep.slax
set groups juniper-ais system scripts op file ais-error.slax
set groups juniper-ais system scripts op file ais-health-report.slax
set groups juniper-ais system scripts op file ais_xfer_jmb.slax
set groups juniper-ais system scripts op file ais_policy_create.slax
```

```

set groups juniper-ais event-options event-script max-datasize 128m
set groups juniper-ais event-options event-script file intelligence-event-main.slax
set groups juniper-ais event-options event-script file bios.slax
set groups juniper-ais event-options event-script file phdc.slax
set groups juniper-ais event-options event-script file Master-event-struct.slax
set groups juniper-ais event-options event-script file Master-event-unstruct.slax
set groups juniper-ais event-options event-script file Master-policy-events.slax
set groups juniper-ais event-options event-script file User-event-struct.slax
set groups juniper-ais event-options event-script file User-event-unstruct.slax
set groups juniper-ais event-options event-script file User-policy-events.slax
set groups juniper-ais event-options event-script file jais-scripts-add.slax
set groups juniper-ais event-options destinations juniper-aim archive-sites
/var/tmp
set apply-groups juniper-ais

```

Service Now provides the following options to install and uninstall AI-Scripts on the managed devices without modifying the device configuration:

- The **Alter device configuration to enable AI-Script events on device** check box on the Install Event Profiles page (as shown in [Figure 49 on page 179](#)) provides the option to install AI-Scripts on a managed device without modifying the device configuration.

This check box is selected by default. To avoid the device configuration from being modified due to installation or upgrade and subsequent commit of AI-Scripts, clear the check box.

Figure 49: Install Event Profile Page

Install Event Profile

Add to Device Group: Default for PHDC

Use Profile: Base_Profile_5_0B1_0

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

☐ Remove Script Bundle files after successful install

☒ Alter device configuration to enable AI-Script events on device

Note:-

1)The 'Alter device configuration' option is enabled by default. This option is applicable only for installing AI-Script release versions 5.0 and above. When selected, Service Now pushes the required configuration (if it is not present on the device) and enable the events.

2) If user does not select the 'Alter device configuration' option, it is expected that user will be pushing the required configuration and enable the events.

3) When installing AI-Script release version pre-5.0, the 'Alter device configuration' option is not applicable. Service Now will always push the configuration for enabling the events as part of the installation.

Please refer the KB Article for more details [KB30464](#)

☐ Schedule at a later time



NOTE:

- If you clear the **Alter device configuration to enable AI-Script events on device** check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device.

For AI-Scripts to be configured and JMBs generated on the device, the static AI-Scripts configuration must be pushed manually and the `/var/db/scripts/op/ais-param-set.slax` file executed on the device.

- When you install or upgrade AI scripts releases earlier than Release 5.0 on a device by using Service Now Release 15.1 or later, the static AI-Scripts configuration must be pushed manually to the device for each installation and upgrade irrespective of whether the **Alter device configuration to enable AI-Script events on device** check box is selected or cleared.

For information about installing AI-Scripts on a device, see [“Installing an Event Profile on a Device by Using Service Now” on page 114](#).

- The **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** option on the Uninstall Event Profiles dialog box as shown in [Figure 50 on page 181](#), when selected, uninstalls AI-Scripts without modifying the device configuration.

This option is cleared by default. When you uninstall AI-Scripts with this option selected, subsequent installation or upgrade of AI-Scripts does not modify the device configuration.

Figure 50: Uninstall Event Profiles Dialog Box



The dialog box is titled "Uninstall Event Profiles" and contains a table for confirming the uninstall of an event profile. The table has two columns: "Host Name" and "Profile Name". The first row shows "srx-220-sn1" and "Test-Latest-5_0". Below the table is a checkbox labeled "Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)". A note section follows, stating that partial uninstall only removes scripts and not configuration, and refers to KB article KB30464. At the bottom are "Submit" and "Cancel" buttons.

Host Name	Profile Name
srx-220-sn1	Test-Latest-5_0

☐ Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)

Note:-
 -Partial Uninstall will only remove scripts but not configuration and some of the related files.
 -Please refer KB article for details [KB30464](#)

Submit **Cancel**



NOTE: If you uninstall AI-Scripts Release 5.0 or later with the Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions) option cleared, ensure that the AI-Scripts configuration on the device is deleted by manually executing the `/var/db/scripts/remove-jais.slax` on the device to avoid errors while committing the AI-Scripts configuration during the next installation or upgrade.

For information about uninstalling AI-Scripts from a device, see “Uninstalling an Event Profile from a Device” on page 117.

Associated Actions

Using the **Event Profiles** task, you can perform the following actions:

- Add an event profile to Service Now; see “Adding an Event Profile to Junos Space Service Now” on page 185 for details.
- Push an event profile to devices; see “Installing an Event Profile on a Device by Using Service Now” on page 114 for details.
- View devices associated with an event profile; see “Displaying Devices Associated with an Event Profile” on page 198 for details.

- Set an event profile as default; see [“Setting an Event Profile as the Default Event Profile in Junos Space Service Now” on page 198](#) for details.
- Import an event profile in XML format; see [“Importing Event Profiles into Junos Space Service Now in XML Format” on page 191](#) for details.
- Export events data to Excel format; see [“Exporting Events Data in Excel Format” on page 199](#) for details.
- Export an event profile in XML format; see [“Exporting Event Profiles from Junos Space Service Now in XML Format” on page 192](#).
- View an event profile; see [“Viewing an Event Profile” on page 195](#) for details.
- Clone an event profile; see [“Cloning an Event Profile” on page 189](#) for details.
- Delete event profiles; see [“Deleting Event Profiles from Junos Space Service Now” on page 194](#) for details.

**Related
Documentation**

- [AI-Scripts Overview on page 27](#)
- [Junos Space Service Now Devices Overview on page 108](#)
- [Incidents Overview on page 232](#)

Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview

Advanced Insight Scripts (AI-Scripts) provide the intelligence that managed devices need to automatically detect and report hardware and software failure or other functional abnormalities. For AI-Scripts to provide intelligence to a device, AI-Scripts must be installed and AI-Scripts configuration committed on a device running Junos OS.

When AI-Scripts are installed, upgraded, or uninstalled on a device, the device configuration is modified. From Service Now Release 15.1R1 or later and AI-Scripts Release 5.0R1 and later, Service Now pushes static AI-Scripts configuration when AI-Scripts are installed on the device for the first time or upgraded to AI-Scripts 5.0 or later for the first time. The static AI-Scripts once committed during the first installation or upgrade to AI-Scripts Release 5.0 or later, is used during the successive installation or upgrade of AI-Scripts on the device. The Static AI-Scripts comprises the following Junos OS commands:

```
set groups juniper-ais system scripts op file ais_change_perm.slax
set groups juniper-ais system scripts op file ais_core_perm.slax
set groups juniper-ais system scripts op file on-demand.slax
set groups juniper-ais system scripts op file remove-jais.slax
set groups juniper-ais system scripts op file ais_arc.slax
set groups juniper-ais system scripts op file ais_attach_file.slax
set groups juniper-ais system scripts op file stop-ais-now.slax
set groups juniper-ais system scripts op file ais_signalSN.slax
set groups juniper-ais system scripts op file ais_core_chm.slax
set groups juniper-ais system scripts op file ais_all_chm.slax
set groups juniper-ais system scripts op file att_signalSN.slax
set groups juniper-ais system scripts op file ais-rsi-chk.slax
set groups juniper-ais system scripts op file ais-param-set.slax
set groups juniper-ais system scripts op file ais-sleep.slax
```

```

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

```

Service Now provides the following options to install and uninstall AI-Scripts on the managed devices without modifying the device configuration:

- The **Alter device configuration to enable AI-Script events on device** check box on the Install Event Profiles page (as shown in [Figure 51 on page 183](#) provides the option to install AI-Scripts on a managed device without modifying the device configuration.

This check box is selected by default. To avoid the device configuration from being modified due to installation or upgrade and subsequent commit of AI-Scripts, clear the check box.

Figure 51: Install Event Profile Page

Install Event Profile

Add to Device Group: Default for PHDC

Use Profile: Base_Profile_5_0B1_0

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

☐ Remove Script Bundle files after successful install

☒ Alter device configuration to enable AI-Script events on device

Note:-

1) The 'Alter device configuration' option is enabled by default. This option is applicable only for installing AI-Script release versions 5.0 and above. When selected, Service Now pushes the required configuration (if it is not present on the device) and enable the events.

2) If user does not select the 'Alter device configuration' option, it is expected that user will be pushing the required configuration and enable the events.

3) When installing AI-Script release version pre-5.0, the 'Alter device configuration' option is not applicable. Service Now will always push the configuration for enabling the events as part of the installation.

Please refer the KB Article for more details [KB30464](#)

☐ ☒ Schedule at a later time

Submit Cancel



NOTE:

- If you clear the Alter device configuration to enable AI-Script events on device check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device.

For AI-Scripts to be configured and JMBs generated on the device, the static AI-Scripts configuration must be pushed manually and the `/var/db/scripts/op/ais-param-set.slax` file executed on the device.

- When you install or upgrade AI scripts releases earlier than Release 5.0 on a device by using Service Now Release 15.1 or later, the static AI-Scripts configuration must be pushed manually to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable AI-Script events on device check box is selected or cleared.

For information about installing AI-Scripts, see [“Installing an Event Profile on a Device by Using Service Now” on page 114](#).

- The **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** option on the Uninstall Event Profiles dialog box as shown in [Figure 52 on page 185](#), when selected, uninstalls AI-Scripts without modifying the device configuration.

This option is cleared by default. When you uninstall AI-Scripts with this option selected, subsequent installation or upgrade of AI-Scripts does not modify the device configuration.

Figure 52: Uninstall Event Profiles Dialog Box



The dialog box is titled "Uninstall Event Profiles" and contains a table for confirming the uninstall of an event profile. The table has two columns: "Host Name" and "Profile Name". The data row shows "srx-220-sn1" for the host name and "Test-Latest-5_0" for the profile name. Below the table, there is a checkbox labeled "Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)". A note section follows, stating that partial uninstall only removes scripts and not configuration, and refers to KB article KB30464. At the bottom are "Submit" and "Cancel" buttons.

Host Name	Profile Name
srx-220-sn1	Test-Latest-5_0

☐ Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)

Note:-
 -Partial Uninstall will only remove scripts but not configuration and some of the related files.
 -Please refer KB article for details [KB30464](#)

Submit **Cancel**



NOTE: If you uninstall AI-Scripts Release 5.0 or later with the Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions) option cleared, ensure that the AI-Scripts configuration on the device is deleted by manually executing the `/var/db/scripts/remove-jais.slax` on the device to avoid errors while committing the AI-Scripts configuration during the next installation or upgrade.

For information about uninstalling AI-Scripts, see "Uninstalling an Event Profile from a Device" on page 117.

Related Documentation

- [Event Profiles Overview on page 177](#)

Adding an Event Profile to Junos Space Service Now

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 Junos Space Service Now" on page 200).

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 53 on page 186](#).

Figure 53: Add Event Profile Page

Add Event Profile

Profile Name:

Description:

Script Bundle: [Add Script Bundle](#)

Find Events: [Show Selected Events](#)

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

1 Page 1 of 1 [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#) [37](#) [38](#) [39](#) [40](#) [41](#) [42](#) [43](#) [44](#) [45](#) [46](#) [47](#) [48](#) [49](#) [50](#) [51](#) [52](#) [53](#) [54](#) [55](#) [56](#) [57](#) [58](#) [59](#) [60](#) [61](#) [62](#) [63](#) [64](#) [65](#) [66](#) [67](#) [68](#) [69](#) [70](#) [71](#) [72](#) [73](#) [74](#) [75](#) [76](#) [77](#) [78](#) [79](#) [80](#) [81](#) [82](#) [83](#) [84](#) [85](#) [86](#) [87](#) [88](#) [89](#) [90](#) [91](#) [92](#) [93](#) [94](#) [95](#) [96](#) [97](#) [98](#) [99](#) [100](#) [101](#) [102](#) [103](#) [104](#) [105](#) [106](#) [107](#) [108](#) [109](#) [110](#) [111](#) [112](#) [113](#) [114](#) [115](#) [116](#) [117](#) [118](#) [119](#) [120](#) [121](#) [122](#) [123](#) [124](#) [125](#) [126](#) [127](#) [128](#) [129](#) [130](#) [131](#) [132](#) [133](#) [134](#) [135](#) [136](#) [137](#) [138](#) [139](#) [140](#) [141](#) [142](#) [143](#) [144](#) [145](#) [146](#) [147](#) [148](#) [149](#) [150](#) [151](#) [152](#) [153](#) [154](#) [155](#) [156](#) [157](#) [158](#) [159](#) [160](#) [161](#) [162](#) [163](#) [164](#) [165](#) [166](#) [167](#) [168](#) [169](#) [170](#) [171](#) [172](#) [173](#) [174](#) [175](#) [176](#) [177](#) [178](#) [179](#) [180](#) [181](#) [182](#) [183](#) [184](#) [185](#) [186](#) [187](#) [188](#) [189](#) [190](#) [191](#) [192](#) [193](#) [194](#) [195](#) [196](#) [197](#) [198](#) [199](#) [200](#) [201](#) [202](#) [203](#) [204](#) [205](#) [206](#) [207](#) [208](#) [209](#) [210](#) [211](#) [212](#) [213](#) [214](#) [215](#) [216](#) [217](#) [218](#) [219](#) [220](#) [221](#) [222](#) [223](#) [224](#) [225](#) [226](#) [227](#) [228](#) [229](#) [230](#) [231](#) [232](#) [233](#) [234](#) [235](#) [236](#) [237](#) [238](#) [239](#) [240](#) [241](#) [242](#) [243](#) [244](#) [245](#) [246](#) [247](#) [248](#) [249](#) [250](#) [251](#) [252](#) [253](#) [254](#) [255](#) [256](#) [257](#) [258](#) [259](#) [260](#) [261](#) [262](#) [263](#) [264](#) [265](#) [266](#) [267](#) [268](#) [269](#) [270](#) [271](#) [272](#) [273](#) [274](#) [275](#) [276](#) [277](#) [278](#) [279](#) [280](#) [281](#) [282](#) [283](#) [284](#) [285](#) [286](#) [287](#) [288](#) [289](#) [290](#) [291](#) [292](#) [293](#) [294](#) [295](#) [296](#) [297](#) [298](#) [299](#) [300](#) [301](#) [302](#) [303](#) [304](#) [305](#) [306](#) [307](#) [308](#) [309](#) [310](#) [311](#) [312](#) [313](#) [314](#) [315](#) [316](#) [317](#) [318](#) [319](#) [320](#) [321](#) [322](#) [323](#) [324](#) [325](#) [326](#) [327](#) [328](#) [329](#) [330](#) [331](#) [332](#) [333](#) [334](#) [335](#) [336](#) [337](#) [338](#) [339](#) [340](#) [341](#) [342](#) [343](#) [344](#) [345](#) [346](#) [347](#) [348](#) [349](#) [350](#) [351](#) [352](#) [353](#) [354](#) [355](#) [356](#) [357](#) [358](#) [359](#) [360](#) [361](#) [362](#) [363](#) [364](#) [365](#) [366](#) [367](#) [368](#) [369](#) [370](#) [371](#) [372](#) [373](#) [374](#) [375](#) [376](#) [377](#) [378](#) [379](#) [380](#) [381](#) [382](#) [383](#) [384](#) [385](#) [386](#) [387](#) [388](#) [389](#) [390](#) [391](#) [392](#) [393](#) [394](#) [395](#) [396](#) [397](#) [398](#) [399](#) [400](#) [401](#) [402](#) [403](#) [404](#) [405](#) [406](#) [407](#) [408](#) [409](#) [410](#) [411](#) [412](#) [413](#) [414](#) [415](#) [416](#) [417](#) [418](#) [419](#) [420](#) [421](#) [422](#) [423](#) [424](#) [425](#) [426](#) [427](#) [428](#) [429](#) [430](#) [431](#) [432](#) [433](#) [434](#) [435](#) [436](#) [437](#) [438](#) [439](#) [440](#) [441](#) [442](#) [443](#) [444](#) [445](#) [446](#) [447](#) [448](#) [449](#) [450](#) [451](#) [452](#) [453](#) [454](#) [455](#) [456](#) [457](#) [458](#) [459](#) [460](#) [461](#) [462](#) [463](#) [464](#) [465](#) [466](#) [467](#) [468](#) [469](#) [470](#) [471](#) [472](#) [473](#) [474](#) [475](#) [476](#) [477](#) [478](#) [479](#) [480](#) [481](#) [482](#) [483](#) [484](#) [485](#) [486](#) [487](#) [488](#) [489](#) [490](#) [491](#) [492](#) [493](#) [494](#) [495](#) [496](#) [497](#) [498](#) [499](#) [500](#) [501](#) [502](#) [503](#) [504](#) [505](#) [506](#) [507](#) [508](#) [509](#) [510](#) [511](#) [512](#) [513](#) [514](#) [515](#) [516](#) [517](#) [518](#) [519](#) [520](#) [521](#) [522](#) [523](#) [524](#) [525](#) [526](#) [527](#) [528](#) [529](#) [530](#) [531](#) [532](#) [533](#) [534](#) [535](#) [536](#) [537](#) [538](#) [539](#) [540](#) [541](#) [542](#) [543](#) [544](#) [545](#) [546](#) [547](#) [548](#) [549](#) [550](#) [551](#) [552](#) [553](#) [554](#) [555](#) [556](#) [557](#) [558](#) [559](#) [560](#) [561](#) [562](#) [563](#) [564](#) [565](#) [566](#) [567](#) [568](#) [569](#) [570](#) [571](#) [572](#) [573](#) [574](#) [575](#) [576](#) [577](#) [578](#) [579](#) [580](#) [581](#) [582](#) [583](#) [584](#) [585](#) [586](#) [587](#) [588](#) [589](#) [590](#) [591](#) [592](#) [593](#) [594](#) [595](#) [596](#) [597](#) [598](#) [599](#) [600](#) [601](#) [602](#) [603](#) [604](#) [605](#) [606](#) [607](#) [608](#) [609](#) [610](#) [611](#) [612](#) [613](#) [614](#) [615](#) [616](#) [617](#) [618](#) [619](#) [620](#) [621](#) [622](#) [623](#) [624](#) [625](#) [626](#) [627](#) [628](#) [629](#) [630](#) [631](#) [632](#) [633](#) [634](#) [635](#) [636](#) [637](#) [638](#) [639](#) [640](#) [641](#) [642](#) [643](#) [644](#) [645](#) [646](#) [647](#) [648](#) [649](#) [650](#) [651](#) [652](#) [653](#) [654](#) [655](#) [656](#) [657](#) [658](#) [659](#) [660](#) [661](#) [662](#) [663](#) [664](#) [665](#) [666](#) [667](#) [668](#) [669](#) [670](#) [671](#) [672](#) [673](#) [674](#) [675](#) [676](#) [677](#) [678](#) [679](#) [680](#) [681](#) [682](#) [683](#) [684](#) [685](#) [686](#) [687](#) [688](#) [689](#) [690](#) [691](#) [692](#) [693](#) [694](#) [695](#) [696](#) [697](#) [698](#) [699](#) [700](#) [701](#) [702](#) [703](#) [704](#) [705](#) [706](#) [707](#) [708](#) [709](#) [710](#) [711](#) [712](#) [713](#) [714](#) [715](#) [716](#) [717](#) [718](#) [719](#) [720](#) [721](#) [722](#) [723](#) [724](#) [725](#) [726](#) [727](#) [728](#) [729](#) [730](#) [731](#) [732](#) [733](#) [734](#) [735](#) [736](#) [737](#) [738](#) [739](#) [740](#) [741](#) [742](#) [743](#) [744](#) [745](#) [746](#) [747](#) [748](#) [749](#) [750](#) [751](#) [752](#) [753](#) [754](#) [755](#) [756](#) [757](#) [758](#) [759](#) [760](#) [761](#) [762](#) [763](#) [764](#) [765](#) [766](#) [767](#) [768](#) [769](#) [770](#) [771](#) [772](#) [773](#) [774](#) [775](#) [776](#) [777](#) [778](#) [779](#) [780](#) [781](#) [782](#) [783](#) [784](#) [785](#) [786](#) [787](#) [788](#) [789](#) [790](#) [791](#) [792](#) [793](#) [794](#) [795](#) [796](#) [797](#) [798](#) [799](#) [800](#) [801](#) [802](#) [803](#) [804](#) [805](#) [806](#) [807](#) [808](#) [809](#) [810](#) [811](#) [812](#) [813](#) [814](#) [815](#) [816](#) [817](#) [818](#) [819](#) [820](#) [821](#) [822](#) [823](#) [824](#) [825](#) [826](#) [827](#) [828](#) [829](#) [830](#) [831](#) [832](#) [833](#) [834](#) [835](#) [836](#) [837](#) [838](#) [839](#) [840](#) [841](#) [842](#) [843](#) [844](#) [845](#) [846](#) [847](#) [848](#) [849](#) [850](#) [851](#) [852](#) [853](#) [854](#) [855](#) [856](#) [857](#) [858](#) [859](#) [860](#) [861](#) [862](#) [863](#) [864](#) [865](#) [866](#) [867](#) [868](#) [869](#) [870](#) [871](#) [872](#) [873](#) [874](#) [875](#) [876](#) [877](#) [878](#) [879](#) [880](#) [881](#) [882](#) [883](#) [884](#) [885](#) [886](#) [887](#) [888](#) [889](#) [890](#) [891](#) [892](#) [893](#) [894](#) [895](#) [896](#) [897](#) [898](#) [899](#) [900](#) [901](#) [902](#) [903](#) [904](#) [905](#) [906](#) [907](#) [908](#) [909](#) [910](#) [911](#) [912](#) [913](#) [914](#) [915](#) [916](#) [917](#) [918](#) [919](#) [920](#) [921](#) [922](#) [923](#) [924](#) [925](#) [926](#) [927](#) [928](#) [929](#) [930](#) [931](#) [932](#) [933](#) [934](#) [935](#) [936](#) [937](#) [938](#) [939](#) [940](#) [941](#) [942](#) [943](#) [944](#) [945](#) [946](#) [947](#) [948](#) [949](#) [950](#) [951](#) [952](#) [953](#) [954](#) [955](#) [956](#) [957](#) [958](#) [959](#) [960](#) [961](#) [962](#) [963](#) [964](#) [965](#) [966](#) [967](#) [968](#) [969](#) [970](#) [971](#) [972](#) [973](#) [974](#) [975](#) [976](#) [977](#) [978](#) [979](#) [980](#) [981](#) [982](#) [983](#) [984](#) [985](#) [986](#) [987](#) [988](#) [989](#) [990](#) [991](#) [992](#) [993](#) [994](#) [995](#) [996](#) [997](#) [998](#) [999](#) [1000](#) [1001](#) [1002](#) [1003](#) [1004](#) [1005](#) [1006](#) [1007](#) [1008](#) [1009](#) [1010](#) [1011](#) [1012](#) [1013](#) [1014](#) [1015](#) [1016](#) [1017](#) [1018](#) [1019](#) [1020](#) [1021](#) [1022](#) [1023](#) [1024](#) [1025](#) [1026](#) [1027](#) [1028](#) [1029](#) [1030](#) [1031](#) [1032](#) [1033](#) [1034](#) [1035](#) [1036](#) [1037](#) [1038](#) [1039](#) [1040](#) [1041](#) [1042](#) [1043](#) [1044](#) [1045](#) [1046](#) [1047](#) [1048](#) [1049](#) [1050](#) [1051](#) [1052](#) [1053](#) [1054](#) [1055](#) [1056](#) [1057](#) [1058](#) [1059](#) [1060](#) [1061](#) [1062](#) [1063](#) [1064](#) [1065](#) [1066](#) [1067](#) [1068](#) [1069](#) [1070](#) [1071](#) [1072](#) [1073](#) [1074](#) [1075](#) [1076](#) [1077](#) [1078](#) [1079](#) [1080](#) [1081](#) [1082](#) [1083](#) [1084](#) [1085](#) [1086](#) [1087](#) [1088](#) [1089](#) [1090](#) [1091](#) [1092](#) [1093](#) [1094](#) [1095](#) [1096](#) [1097](#) [1098](#) [1099](#) [1100](#) [1101](#) [1102](#) [1103](#) [1104](#) [1105](#) [1106](#) [11](#)

Table 20: 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 Junos Space Service Now” on page 200](#)).
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 54: Potential Exposure to Known Issues Page

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

Page 1 of 1 | Displaying 1 - 1 of 1

- (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	The Push to Devices page appears. Here you can select Service Now devices on which you want to install the event profile. For more information, see " Pushing an Event Profile to Devices " on page 195 .
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 195](#)
- [Displaying Devices Associated with an Event Profile on page 198](#)
- [Event Profiles Overview on page 177](#)

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 195.</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 195](#)

- [Event Profiles Overview on page 177](#)

Importing Event Profiles into Junos Space Service Now in XML Format

Junos Space Service Now provides the Import Event Profiles option on the Actions menu of event profiles to import event profiles in the XML format into Service Now. You can import only one XML file at a time. Multiple event profiles can be imported at the same time by including them in the same XML file. Each event profile that is imported is listed on the Event Profiles page.

The following is a sample of the XML file containing event profiles for import into Service Now:

```
<eventProfiles>
  <eventProfile>
    <profileInformation>
      <profileName>Base_profile</profileName>
      <description>Base Profile for Bundle 4.1R1.1</description>
      <scriptBundleVersion>4.1R1.1</scriptBundleVersion>
      <scriptBundleFileName>jais-41.1R1-signed.tgz</scriptBundleFileName>
      <creationTime>[In seconds]</creationTime>
      <userCreated>super</userCreated>
      <eventsIncluded>440</eventsIncluded>
      <eventsExcluded>0</eventsExcluded>
      <deviceInstalled>2</deviceInstalled>
    </profileInformation>

    <scripts>
      <script>
        <scriptId>47</scriptId>
        <eventId>ACCT_MALLOC_FAILURE</eventId>
        <scriptName>ACCT_MALLOC_FAILURE.slax</scriptName>
        <processId>PFED</processId>
        <eventTypeGroup>Resource Exhaustion</eventTypeGroup>
        <eventType>Memory Consumption</eventType>
        <priority>3</priority>
        <userDescription>ACCT_MALLOC_FAILURE</userDescription>
        <eventDescription>The accounting statistics process could not allocate
memory from the heap.</eventDescription>
        <activateDescription>Capture ACCT_MALLOC_FAILURE
Events</activateDescription>
        <featureName>ACCT_MALLOC_FAILURE.slax</featureName>
        <minimumVersion>9.4</minimumVersion>
        <helpText>ACCT_MALLOC_FAILURE</helpText>
        <expressRMA>FALSE</expressRMA>
        <kbUrl>KB18749</kbUrl>
        <platformList>
          <platform>PFE_CHIPSET_ABSENT</platform>
        </platformList>
      </script>
      ...
      ...
    </scripts>
  </eventProfile>
</eventProfiles>
```

To Import event profiles into Service Now in the XML format:

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

The Import Event Profiles page appears as shown in [Figure 55 on page 192](#).

Figure 55: View Event Profiles Page

2. Click **Browse** to browse for the event profile file and click **Upload**.

The event profile is uploaded to Service Now and listed on the Event Profiles page.

Related Documentation

- [Event Profiles Overview on page 177](#)
- [Exporting Event Profiles from Junos Space Service Now in XML Format on page 192](#)

Exporting Event Profiles from Junos Space Service Now in XML Format

Junos Space Service Now provides Export All Profiles and Export Selected Profiles options on the Actions menu of event profiles to export event profiles in the XML format. Export All Profiles exports all the event profiles whereas Export Selected Profiles exports the selected event profiles. All event profiles are exported in a single XML file.

The following is a sample of the exported event profile:

```
<eventProfiles>
  <eventProfile>
    <profileInformation>
      <profileName>Base_profile</profileName>
      <description>Base Profile for Bundle 4.1R1.1</description>
      <scriptBundleVersion>4.1R1.1</scriptBundleVersion>
      <scriptBundleFileName>jais-41.1R1-signed.tgz</scriptBundleFileName>
      <creationTime>[In seconds]</creationTime>
      <userCreated>super</userCreated>
      <eventsIncluded>440</eventsIncluded>
      <eventsExcluded>0</eventsExcluded>
      <deviceInstalled>2</deviceInstalled>
    </profileInformation>

    <scripts>
      <script>
        <scriptId>47</scriptId>
      </script>
    </scripts>
  </eventProfile>
</eventProfiles>
```



```

        <eventId>ACCT_MALLOC_FAILURE</eventId>
        <scriptName>ACCT_MALLOC_FAILURE.s1ax</scriptName>
        <processId>PFED</processId>
        <eventTypeGroup>Resource Exhaustion</eventTypeGroup>
        <eventType>Memory Consumption</eventType>
        <priority>3</priority>
        <userDescription>ACCT_MALLOC_FAILURE</userDescription>
        <eventDescription>The accounting statistics process could not allocate
memory from the heap.</eventDescription>
        <activateDescription>Capture ACCT_MALLOC_FAILURE
Events</activateDescription>
        <featureName>ACCT_MALLOC_FAILURE.s1ax</featureName>
        <minimumVersion>9.4</minimumVersion>
        <helpText>ACCT_MALLOC_FAILURE</helpText>
        <expressRMA>FALSE</expressRMA>
        <kbUrl>KB18749</kbUrl>
        <platformList>
        <platform>PFE_CHIPSET_ABSENT</platform>
        </platformList>
    </script>
    ...
    ...
    ...

</scripts>
</eventProfile>
</eventProfiles>

```

To export event profiles in the XML format:

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

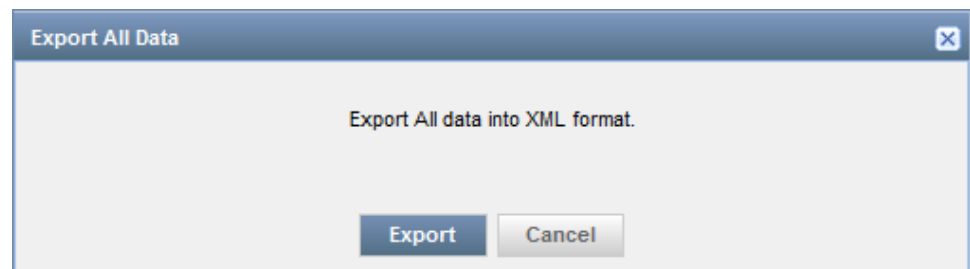
The Event Profiles page appears.

2. On the Event Profiles page, do one of the following:

- To export all event profiles from Service Now, select **Export All Profiles** from the Actions menu. Alternatively, right-click on an event profile and select **Export All Profiles**.

The Export All Data dialog box appears as shown in [Figure 56 on page 193](#).

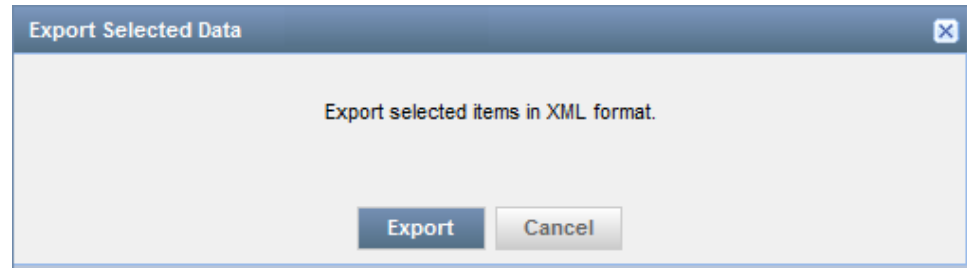
Figure 56: Export All Data Dialog Box



- To export selected event profiles, click the event profiles that you want to export and select **Export Selected Profiles** from the Actions menu. Alternatively, you can click the event profiles that you want to export and select **Export Selected Profiles** from the right-click menu.

The Export All Data dialog box appears as shown in [Figure 57 on page 194](#).

Figure 57: Export All Data Dialog Box



3. Click **Export**.

The Export Job Status dialog box appears. A **Download** link appears on the dialog box to download the XML file after the export job is complete.

4. Click the **Download** link to view or save the XML file on your local system.

**Related
Documentation**

- [Event Profiles Overview on page 177](#)
- [Importing Event Profiles into Junos Space Service Now in XML Format on page 191](#)

Deleting Event Profiles from Junos Space Service Now

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 198](#)
- [Cloning an Event Profile on page 189](#)
- [Pushing an Event Profile to Devices on page 195](#)

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.

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

Related Documentation

- [Exporting Events Data in Excel Format on page 199](#)
- [Cloning an Event Profile on page 189](#)
- [Pushing an Event Profile to Devices on page 195](#)

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:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. 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 58 on page 196](#)).

Figure 58: Push to Devices Dialog Box

Push to Devices

Profile Name: Base_Profile_3_TR1_2
Script Name: jais-3.7R1.2-signed.igz

Select Devices to Install Profile

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle	Event Profile
<input checked="" type="checkbox"/> JCare-Plus	Default for JCare-Plus	device1	PW0213250012	ACX1100	12.3X51-D10.5	3.7R1.2	Base_Profile_3_TR1_2
<input checked="" type="checkbox"/> JCare-Plus	Default for JCare-Plus	device2	JN11B7992AEA	M120	11.4R7.5	3.7R1.2	Profile name
<input checked="" type="checkbox"/> JCare-Plus	Default for JCare-Plus	device3	33108	M101	11.4R7.5	3.7R1.2	Base_Profile_3_TR1_2
<input checked="" type="checkbox"/> JCare-Plus	Default for JCare-Plus	device4	NK0212350232	ACX2100	12.3X52-D10.4		
<input checked="" type="checkbox"/> JCare-Plus	Default for JCare-Plus	device5	AB3510AA0021	SRX3600	11.4R9.4		
<input checked="" type="checkbox"/> JCare-Plus	Default for JCare-Plus	device6	73682	M40E	11.4R7.5		
<input checked="" type="checkbox"/> 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 59: Potential Exposure to Known Issues Page

Potential Exposure when Event Profile is installed on Devices

[Export Devices with Exposure to Excel](#)

	Device Name	Serial Number	Product	Version	Exposure
<input checked="" type="checkbox"/>	 ex-2200-sn3	CW0210403356	EX2200-24T-4G	12.2R3.5	Click

Page

1 of 1

Displaying 1 - 1 of 1

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 198](#)
- [Event Profiles Overview on page 177](#)
- [Adding an Event Profile to Junos Space Service Now on page 185](#)

- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Cloning an Event Profile on page 189](#)
- [Viewing Exposure to Known Issues on page 120](#)

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 195](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)
- [Adding an Event Profile to Junos Space Service Now on page 185](#)
- [Pushing an Event Profile to Devices on page 195](#)

Setting an Event Profile as the Default Event Profile in Junos Space Service Now

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 60 on page 199) shows the default event profile indicated by a unique icon.

Figure 60: View Event Profiles Page

Administration > Event Profiles								
1 Item Selected								
<div>Actions + <input type="text"/></div>								
<input type="checkbox"/>	Name	Description	AI Script Version	Created By	Created +	Events Included	Events Excluded	Devices
<input type="checkbox"/>	Copy of Base_Profile_3_7R1_2	Base Profile for Bundle Version: 3.7R1.2	3.7R1.2	super	Oct 4, 2013 1:26:39 PM IST	433	0	0
<input type="checkbox"/>	Copy of Profile name		3.7R1.2	super	Oct 3, 2013 4:10:58 PM IST	433	0	0
<input type="checkbox"/>	Profile name		3.7R1.2	super	Oct 3, 2013 4:09:06 PM IST	433	0	1
<input checked="" type="checkbox"/>	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 198](#)
- [Cloning an Event Profile on page 189](#)
- [Pushing an Event Profile to Devices on page 195](#)

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 198](#)
- [Cloning an Event Profile on page 189](#)
- [Pushing an Event Profile to Devices on page 195](#)

Adding a Script Bundle to Junos Space 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.

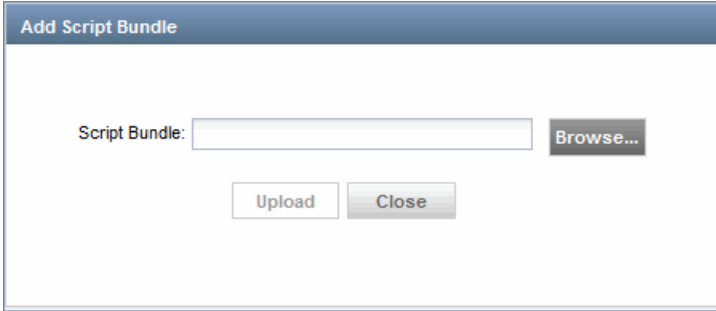
After you add a script bundle to Service Now, to be able to install the script bundle on devices, you must first create an event profile using this script bundle. See [“Adding an Event Profile to Junos Space Service Now” on page 185](#).

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 61 on page 200](#).

Figure 61: Add Script Bundle Dialog Box

A screenshot of the 'Add Script Bundle' dialog box. It has a title bar with the text 'Add Script Bundle'. Inside the dialog, there is a label 'Script Bundle:' followed by a text input field. To the right of the input field is a 'Browse...' button. Below the input field and 'Browse...' button are two buttons: 'Upload' and 'Close'.

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 27](#)
- [Deleting a Script Bundle from Junos Space Service Now on page 201](#)
- [Installing an Event Profile on a Device by Using Service Now on page 114](#)

Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now

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 39](#)
- [Adding a Script Bundle to Junos Space Service Now on page 200](#)
- [Deleting a Script Bundle from Junos Space Service Now on page 201](#)

Deleting a Script Bundle from Junos Space Service Now

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



NOTE: You cannot delete the preloaded 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 27](#)
- [Adding a Script Bundle to Junos Space Service Now on page 200](#)

Global Settings

- [Configuring Global Settings on page 202](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Editing and Deleting an SNMP Configuration on page 206](#)
- [Managing SNMP Traps on page 207](#)
- [Viewing Proxy Server Settings Configured on the Junos Space Platform on page 207](#)
- [Uploading Core Files Generated for Events on page 208](#)

Configuring Global Settings

After installing Junos Space Service Now and configuring it to operate in a specific mode, you must configure the global settings to define purge time for device snapshots, incidents, log files, and BIOS attachments.

To configure Service Now global settings:

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

The Global Settings page appear as shown in [Figure 62 on page 202](#).

Figure 62: Global Settings Page

Global Settings ⓘ

Outbound Email Address: servicenow@juniper.net

Device Snapshot Purge Time (in days): 180

Product Health Data Purge Time (in days): 90

Incident Purge Time (in days): 365

Device Log File Purge Time (in days): 30

Repeat Incident Dampening Period: None

☒ Share Service Now Profile Information

☒ Collect Log Files

Connection Status: OK

Save Test Connection Cancel

2. Enter values for the global settings as described in [Table 21 on page 203](#).
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 21 on page 203 describes the fields displayed on the Global Settings page.

Table 21: Global Settings Parameters

Name	Description	Range/Length	Default
Outbound Email Address	E-mail address that the recipients of e-mails from Service Now see (for example, <code>exampleservicenow@juniper.net</code>)		
Device Snapshot Purge Time (in days)	Number of days device snapshots of a device are stored in the Service Now database before they are deleted	<ul style="list-style-type: none"> • Never • 90 • 120 • 180 • 365 	180
Product Health Data Purge Time (in days)	<p>The number of days the information about product health data (PHD) is stored in Service Now database.</p> <p>Never indicates that the information about PHD is never deleted from the database.</p>	<ul style="list-style-type: none"> • Never • 30 • 45 • 60 • 90 • 120 • 180 • 365 	90
Incident Purge Time (in days)	Number of days the incidents generated for a device are stored in the Service Now database before they are deleted	<ul style="list-style-type: none"> • Never • 90 • 120 • 180 • 365 	365
Device Log File Purge Time (in days)	Number of days the log files collected from a devices are stored in Service Now database before they are deleted.		30
Repeat Incident Dampening Period	<p>The period of time during which Service Now suppresses creation of new incidents on receipt of same JMBs from a device.</p> <p>In other words, if the same event occurs on a device multiple times during the specified time interval, Service Now does not create incidents for each of the occurrences of the event 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 211.</p>	<ul style="list-style-type: none"> • None • Always • 1hr to12hr • 24hr • 48hr • 72hr • 96hr • 120hr 	None

Table 21: Global Settings Parameters (*continued*)

Name	Description	Range/Length	Default
Share Service Now Profile Information	<p>If this check box is selected, all Service Now-related information is shared with JSS for tracking purposes.</p> <p>This option is not available in Offline mode.</p>		Service Now-related information is shared with JSS or Service Now partner.
Collect Log Files	<p>If this check box is selected, log files are collected from all 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.
Connection Status	Status of the connection from Service Now to JSS or Service Now partner.	<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

- [Junos Space Service Now Global Settings Overview](#)
- [Service Now Modes](#)
- [Adding an Organization to Service Now on page 95](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Collecting RSI and System Log Files on page 124](#)
- [Configuring Product Health Data Collection on a Device on page 155](#)

Adding an SNMP Configuration to Service Now

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

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

To add an SNMP server:

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

The SNMP Servers page appears.

2. Click **Add**.

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

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

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

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

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

Loading MIBs

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

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

Related Documentation

- [Configuring Global Settings on page 202](#)
- [Editing and Deleting an SNMP Configuration on page 206](#)
- [Managing SNMP Traps on page 207](#)
- [Notification Policies Overview on page 272](#)

- [SNMP MIBs Downloads](#)

Editing and Deleting an SNMP Configuration

SNMP configurations define the destination for SNMP traps that Service Now sends when a Service Now notification policy is triggered. If you have Service Now Administrator privileges, you can modify the parameters of the SNMP configurations and also delete them.

Editing an SNMP Configuration

To edit an SNMP configuration:

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

The SNMP Configurations 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 Configurations page.

Deleting an SNMP configuration

To delete an SNMP configuration:

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

The SNMP Configurations 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 Configurations page.

Related Documentation

- [Junos Space Service Now Global Settings Overview](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Managing SNMP Traps on page 207](#)
- [SNMP MIBs Downloads](#)

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 63 on page 207](#).

Figure 63: SNMP Trap Attribute Page

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

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

Related Documentation

- [Configuring Global Settings on page 202](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Editing and Deleting an SNMP Configuration on page 206](#)

Viewing Proxy Server Settings Configured on the Junos Space Platform

From Junos Space Service Now Release 14.1 and Junos Space Service Insight Release 14.1, Service Now and Service Insight use the proxy server configured on the Junos Space Network Management Platform to facilitate communication.



NOTE: When upgrading to Service Now Release 14.1, the proxy server configured on Service Now is migrated to the Junos Space Platform if no proxy server is configured on the Junos Space Platform. If a proxy server is already configured on the Junos Space Platform, Service Now uses the proxy server configured on the Junos Space Platform.

To view the proxy server settings that Service Now and Service Insight use, navigate to **Network Management Platform > Administration > Proxy Servers** from the navigation tree. The Proxy Server page lists the configured proxy server.

**Related
Documentation**

- [Configuring Global Settings on page 202](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Editing and Deleting an SNMP Configuration on page 206](#)

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 a fault occurs on a device. You can upload specific core files to Juniper Support System (JSS) either when a case is submitted for an event or after the case is opened for the event. A Service Now end customer can upload core files to the Service Now partner,

To upload core files:

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

The Core File Upload Configuration page appears.

Figure 64: Core File Upload Configuration Page

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 device to FTP server.
- **Disabled-Core Files uploaded manually:** This option enables you to manually upload the core files for a case to JSS.
- **Secure FTP upload through Service Now:** This option enables you to upload core files directly from the device 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 operating in 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 is available to update the credentials from the associated Service Now partner.

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

Related Documentation

- [Organizations Overview on page 93](#)
- [Configuring Global Settings on page 202](#)
- [Administration Overview on page 91](#)
- [Updating Core File Upload Configuration for an End Customer on page 104](#)

Auto Submit Policy

- [Auto Submit Policy Overview on page 210](#)
- [Creating an Auto Submit Policy on page 211](#)
- [Modifying an Auto Submit Policy on page 215](#)
- [Deleting Auto Submit Policies from Service Now on page 216](#)
- [Exporting an Incidents Report on page 216](#)
- [Changing the Status of Auto Submit Policies on page 217](#)
- [Changing the Dampening Status of an Auto Submit Policy on page 218](#)

Auto Submit Policy Overview

An auto submit policy is a policy that you create to enable Service Now to submit incidents to Juniper Support System (JSS) automatically. 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 of the Service Now GUI. 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.

You can dampen events occurring on devices to prevent incidents being created and submitted to JSS for the same event if the event recurs within a configured time period called dampening period. Dampening policy is assigned to individual events. If Auto Submit Policy is activated. You can select a dampening period for which alerts are dampened for an event that recurs on the same device, device group, or organization.

Service Now uses the event ID and synopsis of an event to dampen incident creation. Whenever an event occurs on a device, Service Now checks if an auto submit policy is defined for that event. 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 the event ID and synopsis. If the last event 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 for the event; 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 65 on page 211](#).

Figure 65: 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; see [“Changing the Status of Auto Submit Policies” on page 217](#) for details.
- Export incidents report; see [“Exporting an Incidents Report” on page 216](#) for details.
- Delete auto submit policies; see [“Deleting Auto Submit Policies from Service Now” on page 216](#) for details.
- Modify an auto submit policy; see [“Modifying an Auto Submit Policy” on page 215](#) for details.
- Change dampening status; see [“Changing the Dampening Status of an Auto Submit Policy” on page 218](#) for details.
- Assign an auto submit policy to another domain; see [“Assigning a Service Now Object to a Domain” on page 50](#) for details.

Related Documentation

- [Creating and Editing a Notification Policy on page 274](#)
- [Junos Space Service Now Devices Overview on page 108](#)

Creating an Auto Submit Policy

An auto submit policy enables incidents that are generated on Service Now to be submitted to JSS automatically for creating a Tech Support Case. Although events with priority P1 can be included in an auto submit policy, 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 66 on page 212](#).

Figure 66: Auto Submit Policy Creation Page

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle	Policy
JCare-Plus	Default for JCare-Plus	device1	33108	M10I	11.4R7.5	3.7R1.2	
JCare-Plus	Default for JCare-Plus	device2	PW0213250012	ACX1100	12.3X51-D10.5	3.7R1.2	ASP
JCare-Plus	Default for JCare-Plus	device3	NK0212350232	ACX2100	12.3X52-D10.4		
JCare-Plus	Default for JCare-Plus	device4	JN11B7992AEA	M120	11.4R7.5	3.7R1.2	ASP
JCare-Plus	Default for JCare-Plus	device5	E4008	MX80-48T	11.4R6-S2		
JCare-Plus	Default for JCare-Plus	device6	73682	M40E	11.4R7.5		
JCare-Plus	Default for JCare-Plus	device7	AB3510AA0021	SRX3600	11.4R9.4		

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 Organization** 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
4. Select the devices for which you want to assign the auto submit policy.
 (Optional) To display the list of selected devices to which you want to assign the auto submit policy:
 - a. Click the **Show Selected Devices** link.
 The **Selected Devices** dialog box displays the list of devices that you selected.
 - b. Verify the list and click **Close** to return to the previous page.
5. Click **Next**.
 The **Choose events to include in Auto Submit Policy** page appears.

Figure 67: Choose Events to Include in Auto Submit Policy Page

Administration > Auto Submit Policy > Create Auto Submit Policy









Choose events to include in Auto Submit Policy

Find event:

[Show Selected Events](#)

[Duplicate Incident Dampening](#)

☐ Select All Events Across Pages

Event Synopsis	Type	Sub Type	Dampening (editable)	RMA Event
Category: ACCT (1 Item)				
 ACCT_XFER_POPEN_FAIL	Software Failure	Communication Error	None	No
Category: ALARM (4 Items)				
 CONNECTION_CHASSISD_FAIL	Software Failure	Initialization failure	None	No
 CONNECTION_CRAFTD_FAIL	Software Failure	Initialization error	None	No
 CONNECTION_RTLOGD_FAIL	Software Failure	Initialization error	None	No
 CONNECTION_SEND_ERROR	Software Failure	Process error	None	No
Category: ASP (2 Items)				
 ASP_IDS_INV_CLEAR_QUERY	Software Failure	Unexpected output	None	No
 ASP_IDS_INV_CLEAR_QUERY_VER	Software Failure	Unexpected output	None	No
Category: ASP_L2TP (1 Item)				
 ASP_L2TP_NO_MEM	Resource Exhaustion	Memory Consumption	None	No

Page 1 of 9

Back Next Cancel




Displaying 1 - 50 of 442

6. Select the **Select All Events Across Pages** check box to include all the listed events to the auto submit policy.

You can also manually 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 devices selected in Step 4. You can easily identify these events by looking at the icons that are used to represent them (see Table 22 on page 213).

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 67 on page 213, when you type **audi** in the **Find event** field, all events with names beginning with audi are listed.

Table 22: 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.
	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 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 configured FTP server for 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 the FTP server.
16. In the **Follow Up Method** list, select the method that you would like to use to follow up on the case—Email Full Text Update, Email Secure Web Link, or 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 associated with the auto submit policy, incidents are automatically submitted to Juniper Support system (JSS) and a Tech Support Case is created. For Service Now operating in End Customer mode, the incidents are submitted to Service Now partner.

By default, auto submit policies are enabled. To disable auto submit policies, see [“Changing the Status of Auto Submit Policies” on page 217](#).

Related Documentation

- [Assigning an Auto Submit Policy to a Device on page 133](#)
- [Deleting Auto Submit Policies from Service Now on page 216](#)
- [Exporting an Incidents Report on page 216](#)
- [Changing the Dampening Status of an Auto Submit Policy on page 218](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Creating and Editing a Notification Policy on page 274](#)

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 Configuration to Service Now on page 204](#)
- [Creating and Editing a Notification Policy on page 274](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)

Deleting Auto Submit Policies from Service Now

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 210](#)
- [Creating an Auto Submit Policy on page 211](#)
- [Modifying an Auto Submit Policy on page 215](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)
- [Creating and Editing a Notification Policy on page 274](#)

Exporting an Incidents Report

To export information about incidents associated with 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 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 215](#)
- [Creating and Editing a Notification Policy on page 274](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)

Changing the Status of Auto Submit Policies

Changing the status of an auto submit policy involves enabling or disabling the policy. Incidents can be submitted to Juniper Support System (JSS) only when an auto submit policy is enabled.

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 68 on page 217](#).

Figure 68: Change Auto Submit Policy Status Page

Policy Name	Current Status
ASP	Disabled

☐ Schedule at a later time

Change Status **Cancel**



3. (Optional) Click the **Schedule at a later time** check box and specify a date and time to enable the auto submit policy.
4. Click **Change Status**.

The action is initiated and a Jobs dialog box displays the Job ID. Click the *Job ID* link to view the Jobs page where you can view the status of this action.

5. After the job is complete, click **OK**.

The Quick View of the auto submit policy is displayed in the Auto Submit Policy page.
[Table 23 on page 218](#).

Table 23: 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 215](#)
- [Changing the Dampening Status of an Auto Submit Policy on page 218](#)
- [Auto Submit Policy Overview on page 210](#)
- [Creating an Auto Submit Policy on page 211](#)
- [Creating and Editing a Notification Policy on page 274](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)

Changing the Dampening Status of an Auto Submit Policy

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 69 on page 219](#).

Figure 69: 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

- [Auto Submit Policy Overview on page 210](#)
- [Modifying an Auto Submit Policy on page 215](#)
- [Changing the Status of Auto Submit Policies on page 217](#)
- [Creating an Auto Submit Policy on page 211](#)
- [Creating and Editing a Notification Policy on page 274](#)
- [Adding an SNMP Configuration to Service Now on page 204](#)

Address Group

- [Address Group Overview on page 220](#)
- [Creating an Address Group on page 220](#)
- [Modifying an Address Group on page 221](#)
- [Deleting Address Groups on page 221](#)
- [Associating Devices with an Address Group From the Address Groups Page on page 222](#)
- [Associating Devices with an Address Group From the Organizations Page on page 224](#)
- [Associating Devices with an Address Group from the Device Groups Page on page 225](#)
- [Associating Devices with an Address Group from the Service Now Devices Page on page 226](#)

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 Networks where to ship a particular part in case an RMA case is opened.

A Service Now partner can use the partner address instead of end-customer address when submitting RMA cases for end customers to Juniper Support System (JSS). 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 is 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; see [“Creating an Address Group” on page 220](#) for details.
- Modify an existing address group; see [“Modifying an Address Group” on page 221](#) for details.
- Delete address groups; see [“Deleting Address Groups” on page 221](#) for details.
- Associate address group to a set of devices; see [“Associating Devices with an Address Group From the Address Groups Page” on page 222](#) for details.

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 Organizations page, Device Groups page, and Devices page.

Related Documentation

- [Junos Space Service Now Devices Overview on page 108](#)
- [Organizations Overview on page 93](#)
- [Device Groups Overview on page 105](#)
- [Requesting an RMA Incident on Service Now on page 127](#)

Creating an 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 220](#)
- [Modifying an Address Group on page 221](#)
- [Deleting Address Groups on page 221](#)
- [Associating Devices with an Address Group From the Address Groups Page on page 222](#)

Modifying an 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 220](#)
- [Creating an Address Group on page 220](#)
- [Deleting Address Groups on page 221](#)
- [Associating Devices with an Address Group From the Address Groups Page on page 222](#)

Deleting Address Groups

To delete address groups:

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 220](#)
- [Creating an Address Group on page 220](#)
- [Modifying an Address Group on page 221](#)
- [Associating Devices with an Address Group From the Address Groups Page on page 222](#)

Associating Devices with an Address Group From the Address Groups Page

Using Service Now, you can associate devices with address groups from the Address Groups page.

To associate a device with an address group from the Address Groups page:

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 70 on page 222](#).

Figure 70: Associate Address Group to Devices Page

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-sn1	junos-ex	BM0210329678	ec	Device Group for ec
ex-8200-sn1	junos-ex	CA1710431095	ec	Device Group for ec
ex-4200-sn4	junos-ex	BM0210329621	ec	Device Group for ec

You can associate devices to this address group in any of the following subtypes: 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.

3. 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**.
4. 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 subtype are 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 page, device group page, and device page.

Related Documentation

- [Address Group Overview on page 220](#)
- [Creating an Address Group on page 220](#)
- [Modifying an Address Group on page 221](#)

- [Deleting Address Groups on page 221](#)
- [Associating Devices with an Address Group From the Organizations Page on page 224](#)
- [Associating Devices with an Address Group from the Device Groups Page on page 225](#)
- [Associating Devices with an Address Group from the Service Now Devices Page on page 226](#)

Associating Devices with an Address Group From the Organizations Page

Using Service Now, you can associate devices to address groups from the Organizations page.

To associate a device to an address group from the Organizations page:

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 71: 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		
<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 93](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 222](#)
 - [Associating Devices with an Address Group from the Device Groups Page on page 225](#)
 - [Associating Devices with an Address Group from the Service Now Devices Page on page 226](#)

Associating Devices with an Address Group from the Device Groups Page

Using Service Now, you can associate devices to address groups from the Device Groups page.

To associate a device to an address group from the Device Groups page:

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 72 on page 225](#).

Figure 72: 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 105](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 222](#)
 - [Associating Devices with an Address Group From the Organizations Page on page 224](#)
 - [Associating Devices with an Address Group from the Service Now Devices Page on page 226](#)

Associating Devices with an Address Group from the Service Now Devices Page

Using Service Now, you can associate devices to address groups from the Service Now Devices page.

To associate a device to an address group from Service Now Devices page.

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**
- [Junos Space Service Now Devices Overview on page 108](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 222](#)
 - [Associating Devices with an Address Group From the Organizations Page on page 224](#)
 - [Associating Devices with an Address Group from the Device Groups Page on page 225](#)

E-mail Templates

- [E-mail Templates Overview on page 227](#)
- [Viewing E-mail Templates on page 228](#)
- [Modifying an E-mail Template on page 228](#)

E-mail Templates Overview

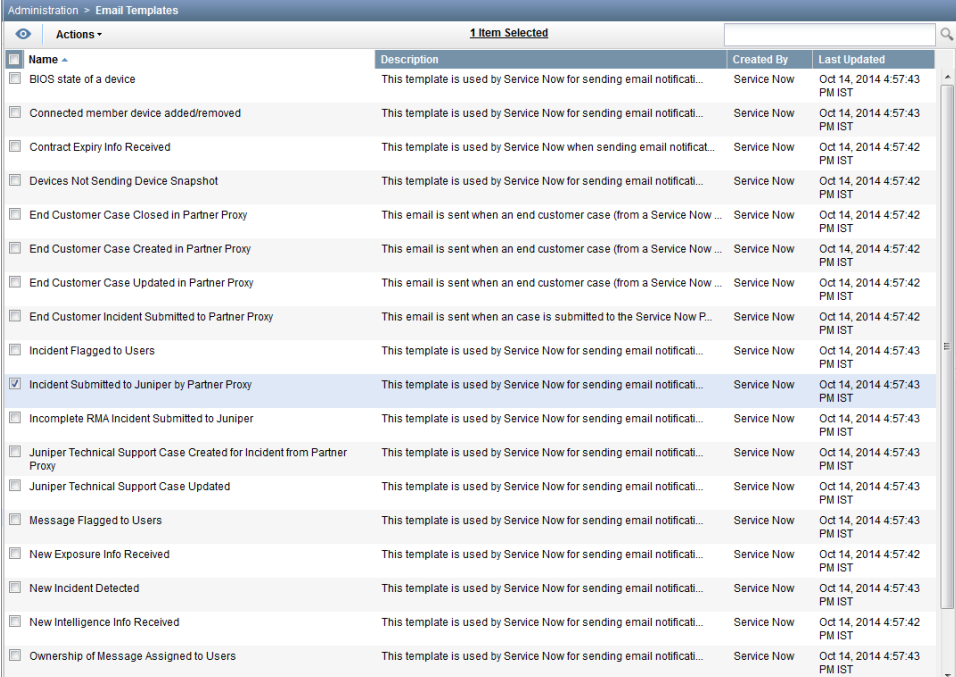
You can use Service Now to send notification for an event through e-mail. Service Now has default e-mail templates whose contents can be modified. However, you cannot modify or delete the default template files. As an administrator, you can update or configure the e-mail content sent to the users during 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 73: E-mail Templates Page



Administration > Email Templates			
Actions		1 Item Selected	
Name	Description	Created By	Last Updated
<input type="checkbox"/> BIOS state of a device	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> Connected member device added/removed	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> Contract Expiry Info Received	This template is used by Service Now when sending email notificat...	Service Now	Oct 14, 2014 4:57:42 PM IST
<input type="checkbox"/> Devices Not Sending Device Snapshot	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:42 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	Oct 14, 2014 4:57:42 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	Oct 14, 2014 4:57:42 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	Oct 14, 2014 4:57:42 PM IST
<input type="checkbox"/> End Customer Incident Submitted to Partner Proxy	This email is sent when a case is submitted to the Service Now P...	Service Now	Oct 14, 2014 4:57:42 PM IST
<input type="checkbox"/> Incident Flagged to Users	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input checked="" type="checkbox"/> Incident Submitted to Juniper by Partner Proxy	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> Incomplete RMA Incident Submitted to Juniper	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 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	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> Juniper Technical Support Case Updated	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> Message Flagged to Users	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> New Exposure Info Received	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:42 PM IST
<input type="checkbox"/> New Incident Detected	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST
<input type="checkbox"/> New Intelligence Info Received	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:42 PM IST
<input type="checkbox"/> Ownership of Message Assigned to Users	This template is used by Service Now for sending email notificati...	Service Now	Oct 14, 2014 4:57:43 PM IST

From the e-mail templates page in Service Now, you can perform the following tasks:

- View e-mail templates; see [“Viewing E-mail Templates” on page 228](#) for details.
- Modify e-mail templates; see [“Modifying an E-mail Template” on page 228](#) for details.

Related Documentation

- [Notification Policies Overview on page 272](#)

- [Creating and Editing a Notification Policy on page 274](#)

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 227](#)
- [Modifying an E-mail Template on page 228](#)

Modifying an E-mail Template

Using Service Now, you can modify the contents of 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 227](#)
- [Viewing E-mail Templates on page 228](#)

CHAPTER 8

Service Central

- [Service Central Overview on page 229](#)
- [Incidents on page 232](#)
- [Technical and End Customer Support Cases on page 251](#)
- [Device Analysis on page 257](#)
- [Information on page 259](#)
- [JMB Errors on page 270](#)
- [Notifications on page 272](#)

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 74: 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*.

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.
- View devices from which BIOS data is collected and the time BIOS data was collected.
- View devices from which product health data is collected and the product health data files collected from the devices.
- 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.
- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

Related Documentation

- [Junos Space Service Now Overview on page 48](#)
- [Service Now Modes](#)
- [Incidents Overview on page 232](#)
- [Device Snapshots Overview on page 264](#)
- [Messages Overview on page 259](#)
- [JMBs with Errors on page 270](#)
- [Notification Policies Overview on page 272](#)
- [Technical and End Customer Support Cases Overview on page 251](#)

Incidents

- [Incidents Overview on page 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Deleting an Incident on page 239](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Uploading an Attachment to an Incident on page 247](#)
- [Updating an End-Customer Case on page 249](#)
- [Uploading Core Files to JSS for an Incident on page 250](#)

Incidents Overview

An incident is the occurrence of a defined event in a device. When an event, 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 event data which is accessed by Junos Space 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 event. The JMB file contains information such as hostname, time stamp of the event, synopsis, description, chassis serial number of the device, and the severity and priority of the event. After a JMB is generated, it is stored at a defined location in the device from where Service Now collects it. For each JMB collected, Service Now creates an incident. The incidents can be viewed on 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.

Table 24 on page 233 lists the fields on the Incidents page.

Table 24: Fields on the Incidents Page

Fields	Description
Organization	The organization associated with the device for which the incident is created.
Device Group	The device group associated with the device for which the incident is created.
Priority	The priority of the incident.
Type	The type of defect.
Incident ID	The ID of the incident.
Incident Type	<p>The type of incident. This parameter can have one of the following values:</p> <ul style="list-style-type: none"> Event—indicates that an event is detected on the Service Now managed devices. On-demand—Indicates that the incident created is an on-demand incident. Event-RMA—indicates that an RMA event is detected on the Service Now managed devices. 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. On-demand RMA—Indicates that the RMA event detected on the device is an on-demand event. AIS Health Check—Indicates the incident is created in response to a JMB collected to obtain information about AI-Scripts error.
Device	The device on which the incident occurred.
Product	The hardware platform the device belongs to.
Occurred	The date and time the incident was created on Service Now.
Total Core Files	The number of core files available for the incident.
Status	The status of the incident.
Flagged	Specifies users are flagged to receive updates about the incident.

You can perform the following tasks from the Incidents page:

- Export JMB to HTML; see [“Exporting a Juniper Message Bundle \(JMB\) to an HTML file” on page 237](#) for details.
- Delete an incident; see [“Deleting an Incident” on page 239](#) for details.
- View JMBs.
- View a Knowledge Base (KB) article pertaining to the incident; see [“Viewing Knowledge Base Articles Associated with an Incident” on page 246](#) for details.

View a case in the Juniper Networks Case Manager; see [“Viewing a Case in Case Manager” on page 254](#) for details.

- Assign the incident to a user; see [“Assigning an Owner to an Incident” on page 234](#) for details.
- Flag an incident to a user; see [“Flagging an Incident to a User” on page 235](#) for details.
- Submit an incident to create a JTAC case; see [“Submitting an Incident to Juniper Support Systems” on page 239](#) for details.
- Export the summary of an incident to Excel; see for details.
- Updating an end customer case; see [“Updating an End-Customer Case” on page 249](#) for details.
- Create auto submit policy for an incident; see for details.
- Upload core files to JSS for incidents; see [“Uploading Core Files to JSS for an Incident” on page 250](#) for details.
- Upload attachments; see [“Uploading an Attachment to an Incident” on page 247](#) for details.



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

- [Checking Incident Status Updates on page 236](#)
- [Viewing Incident Details on page 244](#)
- [AI-Scripts Overview on page 27](#)
- [Service Now Modes](#)
- [Auto Submit Policy Overview on page 210](#)
- [Junos Space Service Now Devices Overview on page 108](#)
- [Notification Policies Overview on page 272](#)

Assigning an Owner to an Incident

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.

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 Details of a Device Snapshot” on page 268](#).

Related Documentation

- [Incidents Overview on page 232](#)
- [Flagging an Incident to a User on page 235](#)
- [Deleting an Incident on page 239](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Deleting an Incident on page 239](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

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 274](#).
- 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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Deleting an Incident on page 239](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

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

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 of the View JMB page in Service Now. However, the option to download the attachments and log files is not available for an exported JMB file.

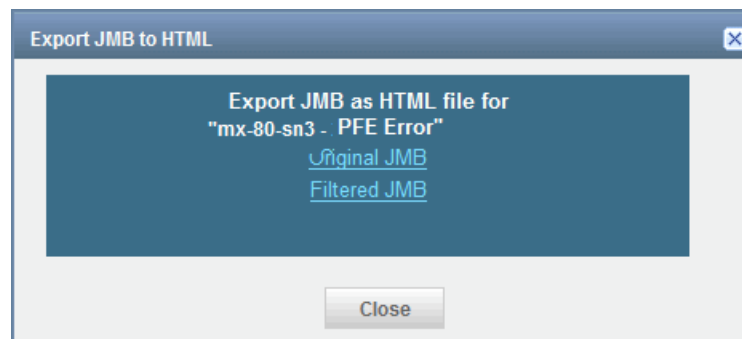
You can export JMBs in the following two formats—HTML and Excel.

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 75 on page 238](#).

Figure 75: 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. On the Incidents page, select the incident whose details you want to export.
3. From the Actions menu, select **Export Incident Summary to Excel**. Alternatively, right-click the incident and select **Export Incident Summary to Excel**.

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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Deleting an Incident on page 239](#)
- [Checking Incident Status Updates on page 236](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

Submitting an Incident to Juniper Support Systems

After viewing the 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 displayed as Submitted.



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.

When a case is created by JSS, the status changes to Created and a case ID is generated for the incident.

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 the 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**.

Figure 76 on page 241 displays the Submit Case Options page cropped up to the Add Comments to the Description field..



NOTE: The Submit Case action is disabled when you select an incident that is already submitted.

Figure 76: Submit Case Options Page

4. Under Email List, 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 the organization.
The username is provided by Juniper Networks or a Juniper Networks partner.
 - b. In the **Password** field, enter the password to log in to the organization.
The password is provided by Juniper Networks or a Juniper Networks partner.

- 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 Direct 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 the 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 the 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 the 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. The Juniper Networks partner has the option of changing this value by selecting an address group present in the partner system.
- If the 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 address group, 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 the 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 Direct 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 name of the core file
- **Core File Size(in bytes)**—Size of the core file, 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 you have uploaded the core files, 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 for which you want to request 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 that appears 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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Deleting an Incident on page 239](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Viewing Incident Details on page 244](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

Viewing Incident Details

An incident is generated in Service Now when an event occurs on a device running Junos OS. An incident includes the following information:

- Incident details: Provides information about the event for which the incident is created—the device on which the event occurred, IP address of the device, the Junos OS version installed on the device, the time of the event, the link to the Knowledge Base for the event, and so on.
- Case details: Provides information about the case generated in Juniper Support Systems (JSS) for the incident—the case ID, site ID, synopsis of the incident, whether the incident was auto submitted to JSS; if auto submitted, the auto submit policy used to auto submit, filter level defined for sharing information with JSS and so on.
- Core file details: Provides information about the core files generated for the event—the path to the core file on the device, the size of the core file in bytes, the time the core file was generated, whether the core file is uploaded to JSS and deleted from the device after copying it to Service Now.



NOTE: For an end customer Service Now, core files are uploaded to the Service Now partner instead of JSS. The core files are uploaded to JSS from Service Now partner.

- Attachment details: Provides information about the attachments generated for the event—the path to the attachment files on the device, the size of the attachment file in bytes, the command used to generate the attachment file, whether the attachment is copied to Service Now and uploaded to JSS.
- Log file details: Provides information about the log files generated for the event—the path to the log file on the device, the size of the log file in bytes, whether the log file is copied to Service Now and uploaded to JSS.

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 77 on page 246](#). The **End-Customer Case Details** tab appears in the partner proxy mode for end customer incidents.

Figure 77: Incident Detail Page

Incident Detail

Incident Details | Case Details | Core File Details | Attachment Details | Log File Details

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: -

KB Article: None

You can retrieve required information from the tabs.

Related Documentation

- [Incidents Overview on page 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Deleting an Incident on page 239](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 246](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)
- [Troubleshooting Issues with Creating Incidents](#)

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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Deleting an Incident on page 239](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Viewing a Case in Case Manager on page 254](#)
- [Updating an End-Customer Case on page 249](#)

Uploading an Attachment to an Incident

Service Now provides the Upload Attachment action for an incident to upload a file, for example, a text, image, or binary file, as an attachment to an incident. Only one file can be uploaded at a time. To upload more than one file, compress the files and upload.



NOTE: We recommend that you limit the size of an attachment to be uploaded to 1 GB and use Secure Copy Protocol (SCP) to upload files of size 1 GB.

The attachment is stored in Service Now if the incident is not submitted to JSS. If a case is already created for the incident, the attachment, when uploaded to the incident is automatically uploaded to the case as well. The attachment uploaded to Service Now can be viewed on the View JMB page of the incident.

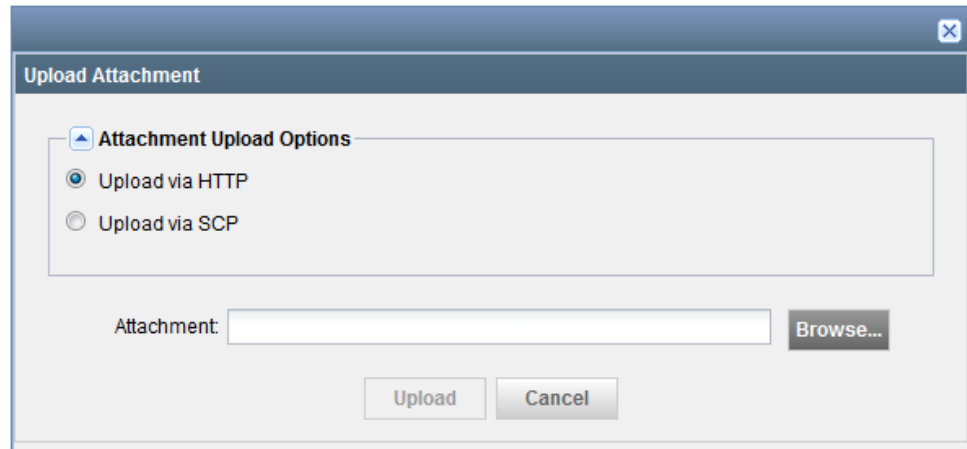
To upload a text or binary attachment to an incident:

1. On the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select an incident for which you want to upload an attachment.

3. From the Actions menu, select **Upload Attachments**. Alternatively, right-click the incident and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in figure.

Figure 78: Upload Attachment Dialog Box



4. Under Attachment Upload Options, do one of the following:
 - Upload an attachment by using HTTP.

To upload an attachment by using HTTP:

 - a. Click **Upload via HTTP**.
 - b. Click the **Browse** button to browse for the attachment file and click **Upload**.

The attachment is uploaded to the incident.
 - Upload an attachment from a remote machine by using SCP.

To upload an attachment by using SCP:

 - a. Click **Upload via SCP**.
 - b. Enter the details of the remote machine hosting the attachment as follows:
 - **Username**: Enter the username of the remote machine.
 - **Password**: Enter the password of the local machine.
 - **Confirm Password**: Retype the password.
 - **Machine IP**: Enter the host IP address of the remote machine.
 - **Software File Path**: Specify the path of the attachment file on the remote machine.
 - c. Click **Submit**.

The process of uploading the attachment is initiated and the File Upload Job information dialog box appears.

After the upload job is complete, you can view the attachment in the JMB associated with the incident.

- Related Documentation**
- [Technical and End Customer Support Cases Overview on page 251](#)
 - [Incidents Overview on page 232](#)
 - [Uploading an Attachment to a Case on page 255](#)

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 79 on page 249](#).

Figure 79: End-Customer Cases Dialog Box

End Customer Cases

Case ID: ECC1

Case Link:

Case Status: Updated ▾

Synopsis: CHASSISD_FRU_OFFLINE_NOTICE

Problem Description: 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

Submit **Cancel**

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**
- [Junos Space Service Now Overview on page 48](#)
 - [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 98](#)
 - [Incidents Overview on page 232](#)
 - [Assigning an Owner to an Incident on page 234](#)
 - [Flagging an Incident to a User on page 235](#)
 - [Deleting an Incident on page 239](#)
 - [Checking Incident Status Updates on page 236](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
 - [Submitting an Incident to Juniper Support Systems on page 239](#)
 - [Viewing Incident Details on page 244](#)
 - [Viewing a Case in Case Manager on page 254](#)

Uploading Core Files to JSS for an Incident

Using Service Now, you can upload core files generated for an event to Juniper Support Systems (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 232](#)

- Submitting an Incident to Juniper Support Systems on page 239
- Uploading Core Files Generated for Events on page 208
- Updating Core File Upload Configuration for an End Customer on page 104

Technical and End Customer Support Cases

- Technical and End Customer Support Cases Overview on page 251
- Viewing a Case in Case Manager on page 254
- Uploading an Attachment to a Case on page 255

Technical and End Customer Support Cases Overview

Technical support cases are created in Junos Space Service Now when incidents generated in Service Now are submitted to Juniper Support System (JSS) and a case ID is assigned to the incidents. You can view the technical support cases on the View Tech Support page of the Service Central workspace.



NOTE: Technical support cases cannot be created when Service Now is operating in Demo mode.

When Service Now is operating in End Customer mode, Service Now can submit incidents only to Service Now partner for opening a technical support case. Service Now cannot directly connect with JSS for submitting incidents.

Figure 80 on page 251 shows the View Technical Support Cases page.

Figure 80: View Tech Support Cases

Organization	Site Id	Device Name	Case ID	Device Serial Number	Time Created	Synopsis	Case Type	Priority	Status
TestOrg	99248		2014-0724-0009	CABV4435	Jul 24, 2014 3:24:33 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0002	CABV4435	Aug 3, 2014 7:54:40 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0003	CABV4435	Aug 3, 2014 8:19:23 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0004	CABV4435	Aug 3, 2014 8:19:42 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0005	CABV4435	Aug 3, 2014 8:28:09 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0006	CABV4435	Aug 3, 2014 10:19:48 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0724-0010	CABV4435	Jul 24, 2014 3:24:43 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0008	CABV4435	Aug 4, 2014 6:33:06 AM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0724-0017	CABV4435	Jul 24, 2014 5:14:07 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0317	CABV4435	Aug 1, 2014 4:42:52 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0318	CABV4435	Aug 1, 2014 4:43:00 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0725-0050	CABV4435	Jul 25, 2014 5:18:08 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0727-0010	CABV4435	Jul 28, 2014 10:15:14 AM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0324	CABV4435	Aug 1, 2014 4:46:38 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0323	CABV4435	Aug 1, 2014 4:44:21 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0326	CABV4435	Aug 1, 2014 4:46:57 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0325	CABV4435	Aug 1, 2014 4:46:54 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0070	CABV4435	Aug 1, 2014 1:03:29 PM IST		Other	2 - High	Open-Initial C

Table 25 on page 252 lists the columns displayed on the View Tech Support Cases page:

Table 25: Fields on the View Tech Support Cases Page

Field	Description
Organization	Organization to which the device for which the case is created belongs
Site ID	Site ID of organization from which the case was submitted This field is not present if Service Now is operating in the End Customer mode.
Device Name	Name of the device for which the case is created
Case ID	ID of the case
Device Serial Number	Serial number of the device for which the case is created
Time Created	Date and time the case was created in JSS
Synopsis	Synopsis of the incident submitted to create the case
Case Type	Type of the case Possible values are: <ul style="list-style-type: none"> • Event—Case created for events that occurred on devices • Event RMA—Case created for Return Materials Authorization (RMA) events that occurred on devices • On-demand—Case created for on-demand incidents • On-demand RMA—Case created for on-demand RMA incidents • BIOS Health Check—Case created for analyzing BIOS running on devices • AIS Health Check—Case created for AI-Scripts health check events on devices • Event (Low End)—Case created for events that occurred on low-end devices such as SRX100 and SRX220 • Other—Case created for events not reported through Service Now
Priority	Priority assigned to the incident, by the end customer, for which the case is created Possible values are: <ul style="list-style-type: none"> • 1 - Critical • 2- High • 3 - Medium • 4 - Low
Status	Status of the case

A Service Now end customer submits incidents to a Service Now partner. The Service Now partner views the incidents submitted by a Service Now end customer in the Incidents page and, if required, submits them to JSS for creating a technical support case. The Service Now partner can view and track the progress of Service Now end-customer cases in the View End Customer Cases page of the Service Central workspace. The Service Now partner updates the status of the case to the Service Now end customer.

Figure 81 on page 253 shows the View End Customer Cases page.

Figure 81: View End Customer Cases Page

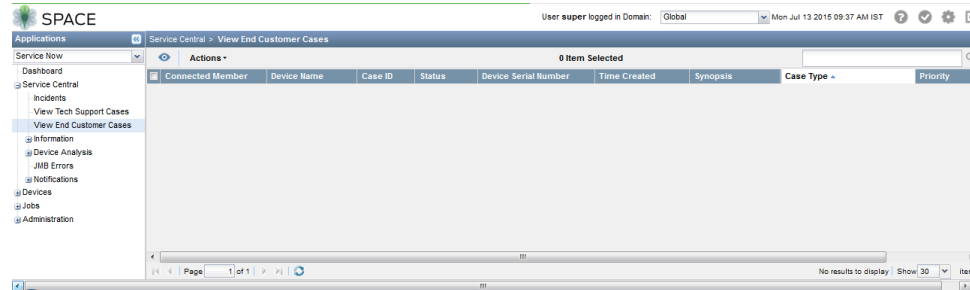


Table 26 on page 253 lists the columns displayed on the View End Customer Cases page:

Table 26: Fields on the View End Customer Cases Page

Field	Description
Connected Member	End customer for whom the case is created
Device Name	Name of the device for which the case is created
Case ID	ID of the case
Status	Status of the case
Device Serial Number	Serial number of the device for which the case is created
Time Created	Date and time the case was created in JSS
Synopsis	Synopsis of the incident submitted to create the case
Case Type	<p>Type of the case</p> <p>Possible values are:</p> <ul style="list-style-type: none"> Event—Case created for events that occurred on devices Event RMA—Case created for Return Materials Authorization (RMA) events that occurred on devices On-demand—Case created for on-demand incidents On-demand RMA—Case created for on-demand RMA incidents BIOS Health Check—Case created for analyzing BIOS running on devices AIS Health Check—Case created for AI-Scripts health check events on devices Event (Low End)—Case created for events that occurred on low-end devices such as SRX100 and SRX220 Other—Case created for events not reported through Service Now

Table 26: Fields on the View End Customer Cases Page (*continued*)

Field	Description
Priority	<p>Priority assigned to the incident, by the end customer, for which the case is created</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low
Related Documentation	<p>You can perform the following tasks from the View Tech Support Cases page:</p> <ul style="list-style-type: none"> • View details of a technical support case in Case Manager; see “Viewing a Case in Case Manager” on page 254 for details. • Add notes to a technical support case; see <i>Adding Notes to a Technical Support Case</i> for details. • Upload binary or text attachments for a technical support case; see “Uploading an Attachment to a Case” on page 255. <p>A Service Now partner can perform the following tasks from the View End Customer Support Cases page:</p> <ul style="list-style-type: none"> • Update an end-customer support case; “Updating an End-Customer Case” on page 249 for details. • View details of an end-customer case in Case Manager; see “Viewing a Case in Case Manager” on page 254 for details.
	<ul style="list-style-type: none"> • Incidents Overview on page 232 • Notification Policies Overview on page 272 • Organizations Overview on page 93 • <i>Junos Space Service Now Global Settings Overview</i>

Viewing a Case in 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 232](#)
- [Assigning an Owner to an Incident on page 234](#)
- [Flagging an Incident to a User on page 235](#)
- [Deleting an Incident on page 239](#)
- [Checking Incident Status Updates on page 236](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 237](#)
- [Submitting an Incident to Juniper Support Systems on page 239](#)
- [Viewing Incident Details on page 244](#)
- [Updating an End-Customer Case on page 249](#)

Uploading an Attachment to a Case

Service Now provides the Upload Attachment option to upload a file, for example, a text, image, or binary file, as an attachment to a case created in Juniper Support System (JSS). Only one file can be uploaded at a time. To upload more than one file, compress the files and upload. The attachments you upload are not stored in Service Now; but, details such as name, type of file, size, and time of upload are stored and can be viewed on the



NOTE:

We recommend that you limit the size of an attachment to be uploaded to 1 GB and use Secure Copy Protocol (SCP) to upload files of size 1 GB.

On a Service Now End Customer, attachments uploaded are stored in the Service Now partner.

To upload a text or binary attachment to an incident:

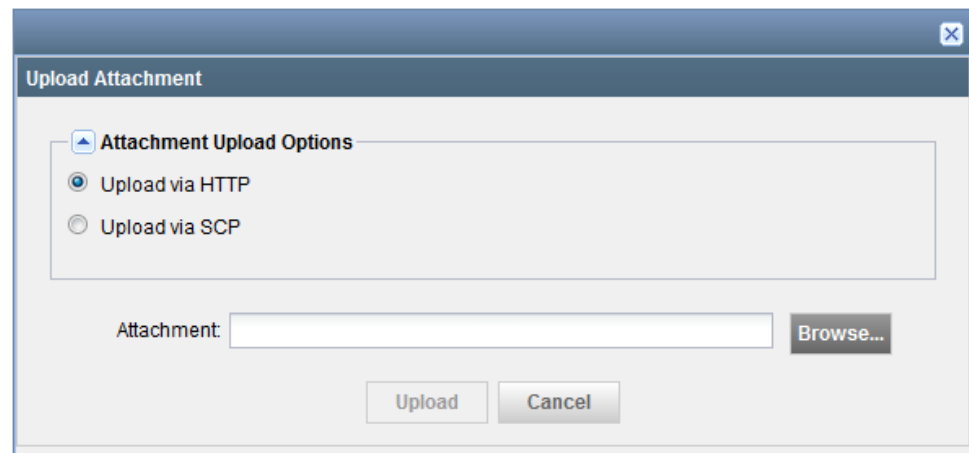
1. On the Service Now navigation tree, select **Service Central > View Tech Support Cases**.

The View Tech Support Cases page appears.

2. Select the technical support case for which you want to upload an attachment.
3. From the Actions menu, select **Upload Attachments**. Alternatively, right-click the technical support case and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in figure.

Figure 82: Upload Attachment Dialog Box



4. Under Attachment Upload Options, do one of the following:

- Upload an attachment by using HTTP.

To upload an attachment by using HTTP:

- a. Click **Upload via HTTP**.
- b. Click the **Browse** button to browse for the attachment file and click **Upload**.

The attachment is uploaded to the incident.

- Upload an attachment by using Secure Copy Protocol (SCP).

To upload an attachment by using SCP:

- a. Click **Upload via SCP**.
- b. Enter the details of the local machine hosting the attachment as follows:
 - **Username:** Enter your username for the local machine.
 - **Password:** Enter your password for the local machine.
 - **Confirm Password:** Retype your password.

- **Machine IP:** Enter the host IP address of the local machine.
 - **Software File Path:** Specify the file path to access the Service Now image file on the local machine.
- c. Click **Submit**.

The process of uploading the attachment is initiated and the File Upload Job dialog box displays the progress of the job.

Related Documentation

- [Technical and End Customer Support Cases Overview on page 251](#)
- [Incidents Overview on page 232](#)
- [Uploading an Attachment to an Incident on page 247](#)

Device Analysis

- [Exporting BIOS Validation Results on page 257](#)
- [Deleting BIOS Validation Results on page 258](#)

Exporting BIOS Validation Results

You can export the results of BIOS validations of managed devices to an Excel file for reference. [Table 27 on page 257](#) lists the BIOS validation information exported to an Excel file.

Table 27: BIOS Validation Field Descriptions

Field Name	Description
Organization	Organization to which the device for which BIOS validation was performed belongs
Device Group	Device group to which the device for which BIOS validation was performed belongs
Connected Member	End customer to which the device belongs; this field is applicable only for a Service Now partner.
Hostname	Hostname of the device from which BIOS data was collected
IP address	IP address of the device from which BIOS data was collected
Entity	Routing Engine of the device for which BIOS validation was performed

Table 27: BIOS Validation Field Descriptions (*continued*)

Field Name	Description
BIOS Result	<p>Status of BIOS validation:</p> <ul style="list-style-type: none"> • Pending Submission—Service Now has received data for BIOS validation from the device; the data is yet to be submitted to Juniper Support System (JSS). • Submitted—Service Now has submitted the BIOS data to JSS for validation. • Submission Failed—Service Now is unable to submit the BIOS validation data of the device to JSS. • Validation Success—Validation of BIOS data by JSS was successful. • Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.
Time Received	Time when the last update of BIOS validation was received from JSS
Junos Version	Version of Junos OS running on the Routing Engine of the device
AI-Scripts Version	Version of AI-Scripts installed on the device

To export BIOS validation results:

1. From the Service Now navigation tree, select **Service Central > Device Analysis > BIOS Validations**.

The BIOS Validations page appears.

2. Select one or more BIOS validation results to be exported.
3. From the Actions menu, select **Export to Excel**. Alternatively, right-click the device and select **Export to Excel**.

The Export BIOS Validations to Excel dialog box appears.

4. Click the **Export the selected BIOS Validations to Excel** link.

The dialog box of the browser to open or save the Excel file appears.

5. Click **Open with** to open the file or click **Save File** to save the file.

Related Documentation

- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 145](#)
- [BIOS Validation Overview on page 141](#)
- [Deleting BIOS Validation Results on page 258](#)

Deleting BIOS Validation Results

You can delete results of BIOS validations when you no longer need them. Junos Space Service Now does not let you delete a BIOS validation result if the status is Pending Case Creation or Case Created. However, on a Service Now end customer, BIOS validations can be deleted irrespective of its status.

To delete BIOS validation results:

1. From the Service Now navigation tree, select **Service Central > Device Analysis > BIOS Validations**.

The BIOS Validations page appears.

2. Select one or more BIOS validation results to be deleted.
3. From the Actions menu, select **Delete BIOS Validations**. Alternatively, right-click the device and select **Delete BIOS Validations**.

The Delete BIOS Validations dialog box appears.

4. Click **Delete** to delete the BIOS validation results or **Cancel** to cancel the deletion.

If you click Delete, the BIOS validation results you selected are no longer listed on the BIOS Validations page.

Related Documentation

- [BIOS Validation Overview on page 141](#)
- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 145](#)
- [Exporting BIOS Validation Results on page 257](#)

Information

- [Messages Overview on page 259](#)
- [Assigning Ownership to Messages on page 260](#)
- [Flagging a Message to Users on page 261](#)
- [Deleting a Message on page 261](#)
- [Assigning a Message to an End Customer on page 262](#)
- [Device Snapshots Overview on page 264](#)
- [Exporting Device Snapshots to HTML on page 265](#)
- [Generating an On-Demand Device Snapshot on page 266](#)
- [Deleting Device Snapshots on page 268](#)
- [Viewing Details of a Device Snapshot on page 268](#)

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, see [“Assigning Ownership to Messages” on page 260](#) for details.
- Assign messages to connected members.
- Flag an information message to users; see [“Flagging a Message to Users” on page 261](#) for details.
- Delete information messages; see [“Deleting a Message” on page 261](#) for details.
- Scan for devices impacted by the message; see *Scanning a Message for Impact* for details.

- Related Documentation**
- [Device Snapshots Overview on page 264](#)
 - [Organizations Overview on page 93](#)

Assigning Ownership to Messages

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 261](#)
 - *Scanning a Message for Impact*
 - [Deleting a Message on page 261](#)
 - [Assigning a Message to an End Customer on page 262](#)
 - [Viewing Messages Assigned to an End Customer on page 103](#)
 - [Messages Overview on page 259](#)
 - [Device Snapshots Overview on page 264](#)

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 264](#)
- [Assigning Ownership to Messages on page 260](#)
- [Scanning a Message for Impact](#)
- [Deleting a Message on page 261](#)
- [Assigning a Message to an End Customer on page 262](#)
- [Viewing Messages Assigned to an End Customer on page 103](#)
- [Messages Overview on page 259](#)

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 264](#)
- [Assigning Ownership to Messages on page 260](#)
- [Flagging a Message to Users on page 261](#)
- [Scanning a Message for Impact](#)
- [Assigning a Message to an End Customer on page 262](#)
- [Viewing Messages Assigned to an End Customer on page 103](#)
- [Messages Overview on page 259](#)

Assigning a Message to an End Customer

Service Now polls Juniper Support System (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*.

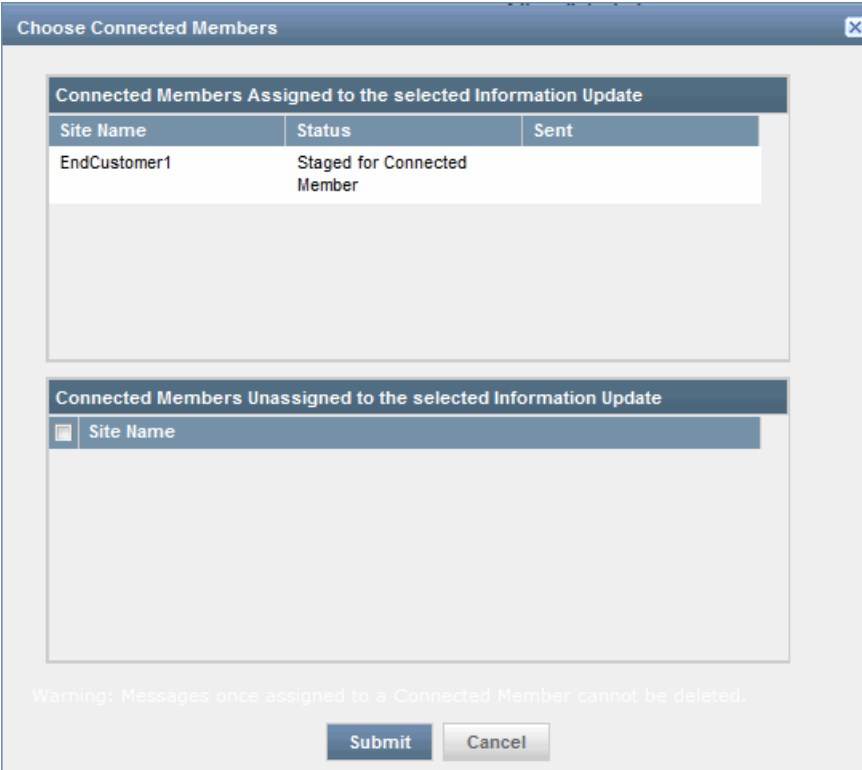
After a message is assigned to a connected member, it cannot be deleted.

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 83 on page 263](#), 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 83: 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 an End Customer”](#) on page 103.

Related Documentation

- [Adding an End Customer to Service Now Configured in Partner Proxy Mode](#) on page 98
- [Device Snapshots Overview](#) on page 264
- [Assigning Ownership to Messages](#) on page 260
- [Flagging a Message to Users](#) on page 261
- [Scanning a Message for Impact](#)
- [Deleting a Message](#) on page 261
- [Viewing Messages Assigned to an End Customer](#) on page 103
- [Messages Overview](#) on page 259

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 to Service Now” on page 95](#)) 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; see [“Exporting Device Snapshots to HTML” on page 265](#) for details.
- Delete a device snapshot; see [“Deleting Device Snapshots” on page 268](#) for details.
- View device snapshot details; see [“Viewing Details of a Device Snapshot” on page 268](#) for details.

Related Documentation

- [Messages Overview on page 259](#)
- [Monitoring Device Snapshots](#)
- [Adding an Organization to Service Now on page 95](#)
- [AI-Scripts Overview on page 27](#)

Exporting Device Snapshots 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 264](#)
 - [Deleting Device Snapshots on page 268](#)
 - [Viewing Details of a Device Snapshot on page 268](#)
 - [Messages Overview on page 259](#)

Generating an On-Demand Device Snapshot

Junos Space Service Now provides the *Create On-Demand Device Snapshots* action for managed devices to generate off-box on-demand device snapshots or informational Juniper Message Bundles (iJMBs) on managed devices. You can choose to automatically upload the iJMB to Juniper Support System (JSS) or the Service Now partner (in case Service Now is operating in the End Customer mode).

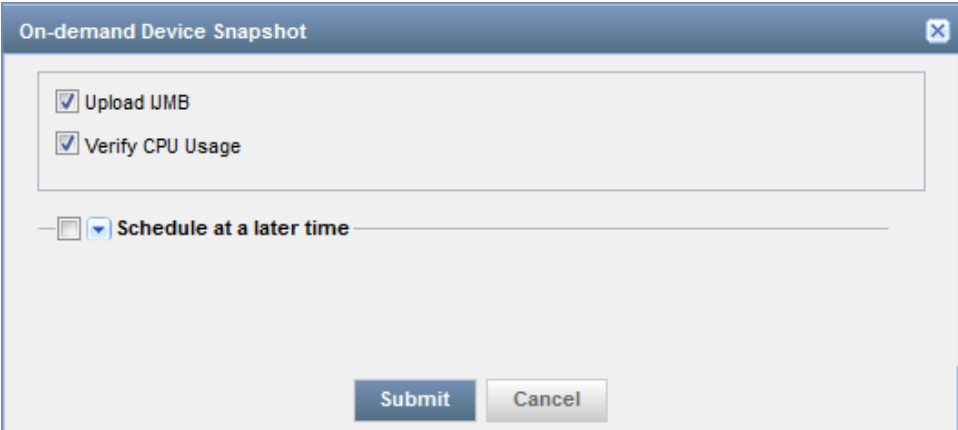
To generate an on-demand device snapshot:

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 **Device Operations > Create On-Demand Device Snapshots**. Alternatively, right-click the device and select **Device Operations > Create On-Demand Device Snapshots**.

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

The On-demand Incident dialog box appears as shown in [Figure 84 on page 266](#).

Figure 84: On-demand Incident Dialog Box

The image shows a dialog box titled "On-demand Device Snapshot". It has a close button (X) in the top right corner. Inside the dialog, there are two checked checkboxes: "Upload iJMB" and "Verify CPU Usage". Below these, there is a section with a minus icon, a dropdown arrow, and the text "Schedule at a later time". At the bottom of the dialog, there are two buttons: "Submit" and "Cancel".

4. (Optional) Clear the **Upload iJMB** check box to prevent the iJMB from being uploaded to Juniper Support System (JSS).

By default, the check box is selected and iJMBs are automatically uploaded to JSS.

5. (Optional) Clear the **Verify CPU Usage** check box to avoid checking the load average value and ideal time of the device CPU before generating the iJMB.

By default, this check box is selected. If the average load and ideal time of the CPU are not within the limits defined in [Table 28 on page 267](#), the off-box on-demand JMB is not generated and an error message is displayed. Service Now determines the CPU load average from the output of the **get-system-uptime-information** command and the CPU idle time from the output of the **get-route-engine-information** command.

Table 28: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs

Device	CPU Load Average	CPU Ideal Time
MX240, MX480, MX960, MX120, MX320	< 2	> 15
Other Supported Devices	< 1	> 15

6. (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 to schedule the iJMB generation.
7. Click **Submit**.
- A Job Information dialog box that appears displays the job ID as a link.
8. Click the *job ID* link to go to the Create on-demand Device Snapshot job on the Jobs page.
9. Double-click the job to open the Create On-demand Incident Status dialog box to view the status of the create on-demand device snapshot job.

Related Documentation

- [Junos Space Service Now Devices Overview on page 108](#)
- [Assigning an Auto Submit Policy to a Device on page 133](#)
- [Generating an On-Demand Incident on page 121](#)
- [Requesting an RMA Incident on Service Now on page 127](#)
- [Collecting RSI and System Log Files on page 124](#)

Deleting Device Snapshots

Service Now collects and displays device snapshots or iJMBs collected from devices on the Device Snapshots page. Device snapshots are by default stored for 180 days in the Service Now database. The number of days the device snapshots can be stored is configured on the Device Snapshot Purge Time (in days) parameter on the Global Settings page.

Service Now provides the Delete option on the Actions menu for a device snapshot to delete it when required.

To delete a device snapshot:

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

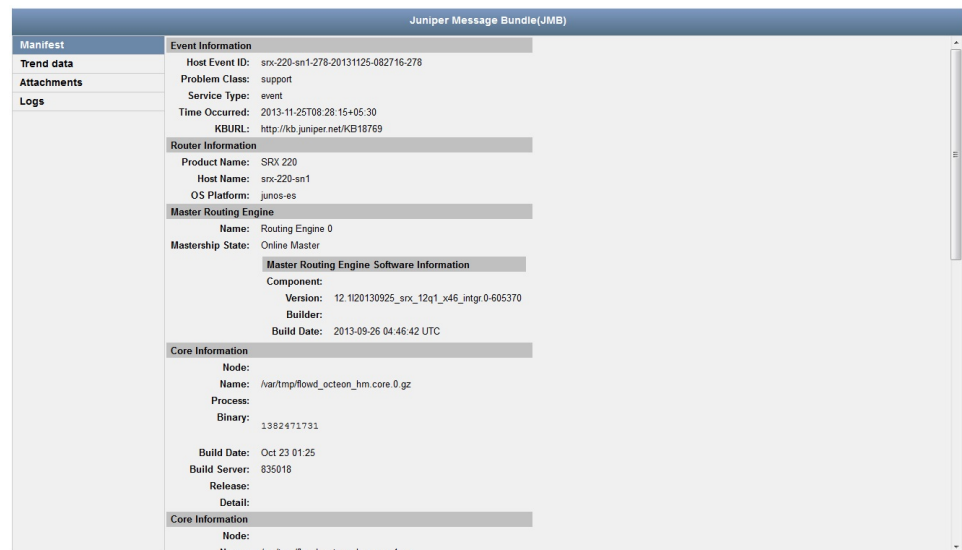
- [Device Snapshots Overview on page 264](#)
- [Exporting Device Snapshots to HTML on page 265](#)
- [Viewing Details of a Device Snapshot on page 268](#)
- [Messages Overview on page 259](#)
- *Junos Space Service Now Global Settings Overview*

Viewing Details of a Device Snapshot

When Service Now receives informational JMBs or iJMBs, 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 85 on page 269](#). You can click the links in the Attachments and Logs sections to view or download attachments and system log files.

Figure 85: Juniper Message Bundle



To view details of a JMB:

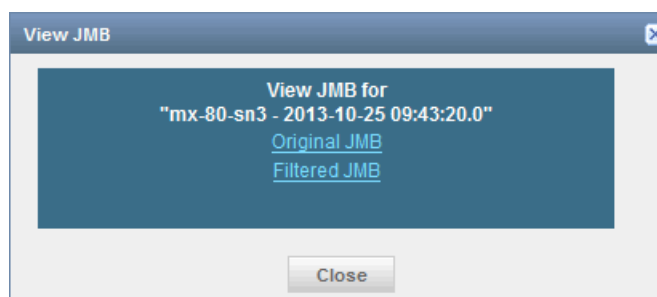
1. From the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.

The Device Snapshots page appears.

2. On the Device Snapshots page, select the device for which you want to view an iJMB.
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 86 on page 269. The information in the filtered JMB is classified by the settings on your Global Settings page.

Figure 86: View JMB Dialog Box



4. Click the **Original JMB** or **Filtered JMB** link to view the JMB details.

Clicking Original JMB displays the JMB as received from the device. Clicking Filtered JMB displays the JMB after filtering data as configured in the filter criteria.

Related Documentation

- [Device Snapshots Overview on page 264](#)
- [Exporting Device Snapshots to HTML on page 265](#)
- [Deleting Device Snapshots on page 268](#)
- [Messages Overview on page 259](#)

JMB Errors

- [JMBs with Errors on page 270](#)

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 Data section or an incomplete attachment in the Attachment section 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 270](#)
- [Deleting JMBs with Errors on page 271](#)

Downloading JMBs with Errors

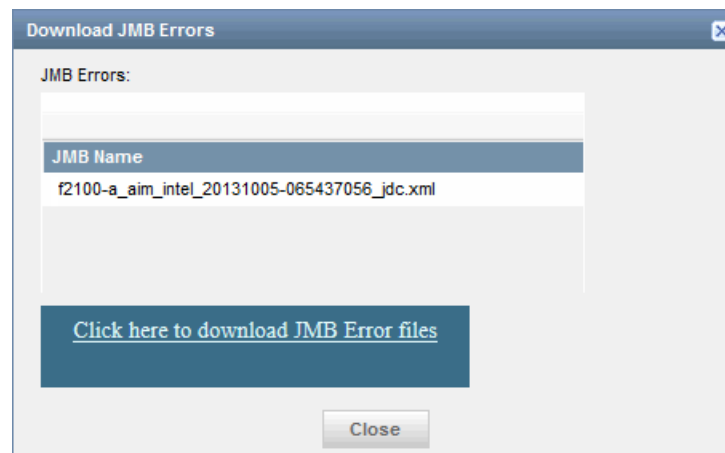
When you download a JMB, it is saved as a zip file. You can download up to five JMBs with errors at a time.

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 87 on page 271](#).

Figure 87: 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 JMBs with errors are deleted from the Service Now database and they no longer appear on the JMB Errors page.

- Related Documentation**
- [Service Central Overview on page 229](#)
 - [Messages Overview on page 259](#)

Notifications

- [Notification Policies Overview on page 272](#)
- [Creating and Editing a Notification Policy on page 274](#)
- [Enabling or Disabling a Notification Policy on page 281](#)
- [Deleting a Notification Policy on page 281](#)

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 on Service Now 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**—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.

[Table 29 on page 272](#) lists the triggers and filters that can be configured on Service Now.

Table 29: Notification Triggers and Trigger Filters

Trigger	Description	Filters
New Incident Detected	<p>Trigger to send a notification when a new incident is received from a Service Now Device.</p> <p>This is the only option available when Service Now is in offline mode.</p>	Priority, Organization, Device groups, Device name, Serial number, Has the words, and Does not have
Incident Submitted	Trigger to send a notification when an incident is submitted to JSS for creating a case	Priority, Organization, Device group, Device name, Serial number, Has the words, and Does not have
Case ID Assigned	Trigger to send a notification when a case ID is assigned to an incident in Juniper Support System (JSS)	Priority, Organization, Device groups, Device name, Serial number, Has the words, and Does not have
Case Status Updated	Trigger to send a notification when the status of a case is updated	Priority, Organization, Device groups, Device name, Serial number, Has the words, and Does not have
New Intelligence Update	Trigger to send a notification when one or more device snapshots or informational JMBs are received	Intelligence update type, Products affected, Platform type, Keywords, Serial Number, Software Version, Organization, Device Group, Devices impacted, Has the words, Does not have

Table 29: Notification Triggers and Trigger Filters (*continued*)

Trigger	Description	Filters
Service Contract Expiring	<p>Trigger to send a notification when the technical support contract license is nearing expiry for one or more devices</p> <p>The notification is sent sixty days before expiry of the service contract and lists devices for which the technical support contract is nearing expiry</p>	Organization, Device group, Device name, Serial number
New Exposure	Trigger to send a notification when one or more managed devices are susceptible to known issues	Organization, Device group, Devices
Ship-to Address Missing For Device	Trigger to send a notification when an RMA incident is submitted to Juniper Support Systems without ship-to address	Priority, Organization, Device group, Device name, Serial number, Has the words, Does not have
Switch over enabled for iJMB	<p>Trigger to send a notification when Service Now switches over to auto collection mode for collecting iJMBs (Device Snapshot) for one or more managed devices</p> <p>Service Now switches iJMB collection to auto collection mode when it does not receive iJMBs even though AI-Scripts is installed on the device.</p>	Organization, Device group, Device name, Serial number, Products, Platform type
PHD Collection Failure	Trigger to send a notification when Service Now fails to collect product health data (PHD) from one or more managed devices	Organization, Device group, Device name, Serial number, Send email for every
Connected Member Device Added/Removed	Trigger to send a notification by a Service Now operating in Partner Proxy mode when a device is added or removed by an end customer	Connected member, Device name, Serial number, State

From the Notifications page, you can perform the following actions:

- Edit filters and actions configured for a trigger; see [“Creating and Editing a Notification Policy” on page 274](#) for details.
- Enable or disable a notification policy; see [“Enabling or Disabling a Notification Policy” on page 281](#) for details.
- Delete a notification policy; see [“Deleting a Notification Policy” on page 281](#) for details.

Related Documentation

- [Incidents Overview on page 232](#)
- [Technical and End Customer Support Cases Overview on page 251](#)
- [Messages Overview on page 259](#)
- [Device Snapshots Overview on page 264](#)
- [BIOS Validation Overview on page 141](#)
- [Product Health Data Collection Overview on page 147](#)
- [E-mail Templates Overview on page 227](#)

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 88 on page 274](#),

Figure 88: Create Notifications Page

The screenshot shows the 'Create Notifications' page. At the top, the title is 'Create Notifications'. Below the title, there are two input fields: 'Name' with the value 'RMA Addrss Missing' and 'Trigger' with a dropdown menu showing 'New Incident Detected'. Below these is a section titled 'Apply Filters' which is expanded. It contains several filter fields: 'Priority' (None), 'Organization' (None), 'Device Group' (None), 'Device Name', 'Serial Number', 'Has the words', and 'Does not have'. Below the filters is the 'Actions' section. It contains a table titled 'Send SNMP Traps to' with two columns: 'Name' and 'SNMP-Partner'. The table has one row with 'SNMP-Partner' checked. There are 'Add' and 'Cancel' buttons at the bottom right of the 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 30 on page 275](#).

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 30 on page 275](#).

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 30 on page 275](#).

Table 30: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Remark
Name	Enter a unique name for the policy.	64 characters	—

Table 30: 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.
		Partner Certificate Expiry	Notifications are sent when the SSL certificate of the partner is about to expire.

Table 30: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
		Connected Member Device Added/Removed	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 30: 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 30: 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
Filter Parameters for BIOS Information Updates Trigger:			
Organization	Service Now sends a notification if the organization associated with the device the incident occurred on matches the value entered in this field.		
Device Group	Service Now sends a notification if the device group associated with the device the incident occurred on matches the value entered in this field.		
Device Name	Service Now sends a notification if the name of the device the incident occurred on matches the value entered in this field.		
Serial Number	Service Now sends a notification if the serial number of the device the incident occurred on matches the value entered in this field.		

Table 30: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
BIOS Status	<p>Select a value for the BIOS status. BIOS status indicates the status of BIOS validation.</p> <p>Service Now sends a notification if the BIOS status matches the value selected in this field.</p>	<ul style="list-style-type: none"> Both—a notification is sent irrespective of whether the BIOS validation succeeds or fails. Success—a notification is sent only if the BIOS validation succeeds. Failure—a notification is sent only if the BIOS validation fails. 	
Filter Parameters for PHD Collection Failure Trigger:			
Organization	<p>Select an organization from the drop-down list.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device belonging to the organization.</p>		
Device Group	<p>Select a device group from the drop-down list.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device belonging to the device group.</p>		
Device Name	<p>Enter a device name.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device with the entered device name.</p>		
Serial Number	<p>Enter a serial number.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device with the entered serial number.</p>		
Send Email for every	<p>Select a value from the drop-down list.</p> <p>Service Now send a notification when it fails to collect PHD files from a device for the selected number of hours.</p>	<ul style="list-style-type: none"> 1 Hour 6 Hours 12 Hours 24 Hours 	The default value is 6 hours.
Actions:			
Send Email to	<p>Specify the e-mail addresses of users who must receive an alert if the policy is triggered and matches the specified filter.</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	Blank

Table 30: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
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 Configuration to Service Now” on page 204 .	–	–

- Related Documentation**
- [Notification Policies Overview on page 272](#)
 - [Enabling or Disabling a Notification Policy on page 281](#)
 - [Deleting a Notification Policy on page 281](#)

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 272](#)
 - [Creating and Editing a Notification Policy on page 274](#)
 - [Deleting a Notification Policy on page 281](#)
 -

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 272](#)
- [Creating and Editing a Notification Policy on page 274](#)
- [Enabling or Disabling a Notification Policy on page 281](#)

PART 3

Junos Space Service Insight

- [Introduction to Service Insight on page 285](#)
- [User Roles on page 291](#)
- [Insight Central on page 293](#)

CHAPTER 9

Introduction to Service Insight

- [Service Insight Overview on page 285](#)

Service Insight Overview

- [Service Insight Overview on page 285](#)
- [Service Insight Domain Overview on page 289](#)

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 to Service Now” on page 95](#) 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 294](#).

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 309](#).

Juniper Care Plus (JCare 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 matched 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 from JSS. 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 314](#).

Service Insight uses two timers, one that runs every midnight, and another that runs every hour. The timers initiate the process to fetch EOL data of devices from JSS.

When a large number of devices is added to Service Insight, EOL data is received by Service Insight 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. If the device information in Service Now and Service insight are not synchronized, the midnight timer initiates a synchronization process so that changes made to devices in Service Now are reflected in Service Insight.

- [Service Insight Dashboard on page 286](#)
- [Dashboard Gadgets on page 287](#)

Service Insight Dashboard

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 286](#)

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 31 on page 287](#) lists the tasks that can be performed using the Service Insight workspaces.

Table 31: 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

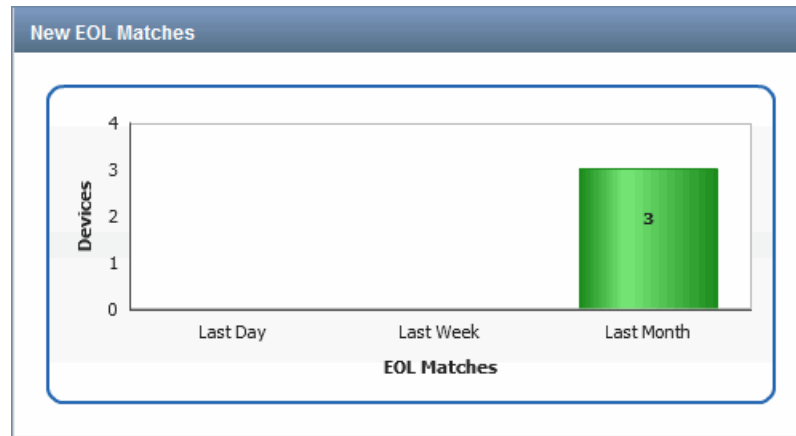
The dashboard displays gadgets with information that is updated automatically and instantaneously. You can move gadgets on the dashboard and change their sizes. These changes persist even after you log back in to the system. The gadgets displayed on the Service Insight dashboard are:

- [New EOL Matches on page 287](#)
- [Recent PBNs on page 288](#)
- [PBN Severity on page 288](#)
- [Service Insight Notices on page 289](#)

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.

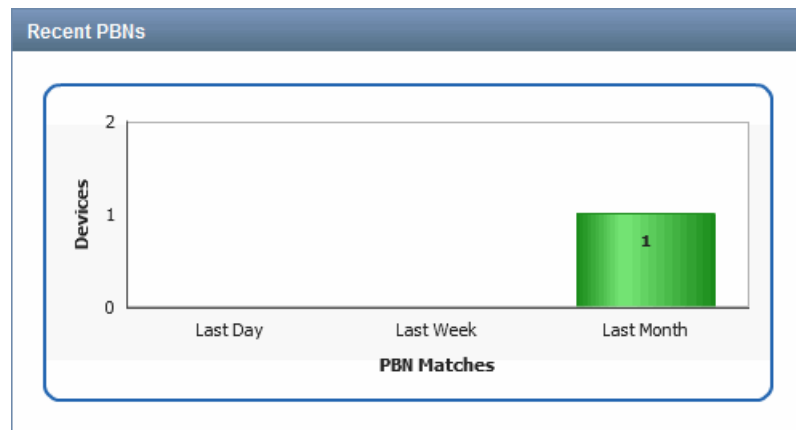
For example, when you click the green bar of the **New EOL Matches** gadget (as shown in the following figure), the **Exposure Analyzer** page displays only the two devices for which EOL notifications were received last month.



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.

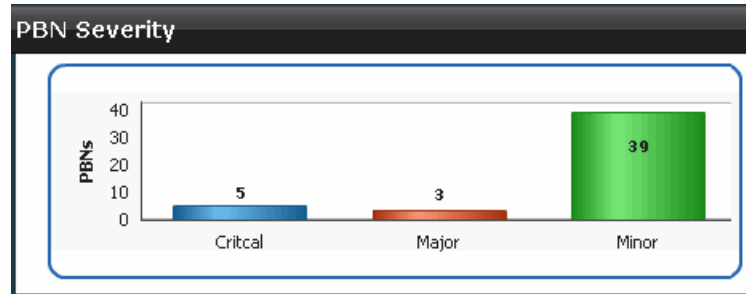
For example, when you click the green bar of the **Recent PBNs** gadget (as shown in the following figure), the **Manage PBNs** page lists only those three devices for which PBNs were received last month.



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 293](#)
- [Service Insight Domain Overview on page 289](#)

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* at [Junos Space Network Management Platform Documentation](#).

When you access Service Insight, only the EOL report, PBN report, and notification objects that 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 the objects in them by selecting the domains from the **Login as username in** list on the banner of the Junos Space GUI. Only the domains to which you are assigned are listed in the **Login as username in** list. A super user can access all domains.

EOL report, PBN report, and notification objects that you create when you are logged in to a certain domain are assigned to that domain. If needed, you can assign these objects to another domain. For information about assigning an object to another domain, see [“Assigning a Service Insight Object to Another Domain” on page 290](#).

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 domains and cannot be assigned to another domain. [Table 32 on page 290](#) lists Service Insight objects and their default domains.

Table 32: 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 to which a user is logged in	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:

- From the Service Insight navigation tree, select the object.
The object's page appears.
- On the object's page, select the object's instance that you want to assign to another domain.
You can select multiple instances of the object to assign to another domain.
- 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.
- 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 inventory landing page.
- 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 Service Insight GUI is refreshed.
- 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 293](#)
 - [Administration Overview on page 91](#)
 - [Domains Overview](#)

CHAPTER 10

User Roles

- [Junos Space Service Insight User Roles on page 291](#)

Junos Space Service Insight 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 33 on page 291](#) for the list of predefined user roles available in Service Insight. All the roles are applicable in the Insight Central workspace of the Service Insight application.

Table 33: Predefined Roles for the Service Insight Application

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

Table 33: Predefined Roles for the Service Insight Application (*continued*)

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

To create and manage users, on the Junos Space Network Management Platform GUI, select **Network Management Platform > Role Based Access Control > User Accounts**. The User Accounts page lists the existing users. Use this page to create and assign roles to Service Now and Service Insight users.

For information about creating users, see *Creating Users in Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide* available at

http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html.

**Related
Documentation**

- *User Roles and Permissions Overview*
- [Insight Central Overview on page 293](#)
- *Creating Users in Junos Space Network Management Platform*

CHAPTER 11

Insight Central

- [Insight Central Overview on page 293](#)
- [Exposure Analyzer on page 294](#)
- [Managing EOL Reports on page 300](#)
- [Managing PBN Reports on page 305](#)
- [Managing PBNs on page 309](#)
- [Managing Notifications on page 313](#)

Insight Central Overview

- [Insight Central Overview on page 293](#)

Insight Central Overview

- [Insight Central Overview on page 293](#)

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 to Service Now” on page 95](#).

The Insight Central landing page (as shown in [Figure 89 on page 294](#)) 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 89: Insight Central Landing Page



Related Documentation

- [Service Insight Overview on page 285](#)
- [Exposure Analyzer Overview on page 294](#)
- [EOL Reports Overview on page 300](#)
- [PBN Reports Overview on page 305](#)
- [Targeted PBNs Overview on page 309](#)
- [Notifications Overview on page 314](#)

Exposure Analyzer

- [Exposure Analyzer on page 294](#)

Exposure Analyzer

- [Exposure Analyzer Overview on page 294](#)
- [Generating EOL Reports on page 296](#)
- [Generating PBN Reports on page 297](#)
- [Showing Matching PBNs on page 300](#)

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 90 on page 295](#)). 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 34 on page 295](#) describes these icons. [Table 35 on page 296](#) 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: devices with End of Life announce parts, serial number of the device, model number of the device, top level assembly part for the device, End of Sale date, and End of Service date, Last Hardware Engineering Support date, Last Software Engineering Support date 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 90: 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 34 on page 295 describes the icons on the exposure analyzer page.

Table 34: Exposure Analyzer Page Icon Descriptions



Icon	Description
	An EOL report is received for the device
	A PBN is received for the device.

Table 35 on page 296 describes the fields on the Exposure Analyzer page and the Device Details dialog box.

Table 35: 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 296.](#)
- [Generating PBN Reports on page 297](#)
- [“Showing Matching PBNs” on page 300.](#)

Related Documentation

- [Targeted PBNs Overview on page 309](#)
- [Notifications Overview on page 314](#)

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, Last Software Engineering Support date, number of Last Software Engineering Support parts, Last Hardware Engineering Support date, number of Last Hardware Engineering Support parts, End of Sale date, End of Service date, 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 300](#)
- [Regenerating EOL Reports on page 304](#)

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

The **Generate PBN Report** dialog box appears as shown in [Figure 91 on page 298](#).

Figure 91: Generate PBN Report Dialog Box

Generate PBN Report

☐ Do not save this report on Service Insight

Enter PBN Report Name:

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

Device Name	PBN Matches
Device1	Yes
Device2	Yes
Device3	Yes

Send Email To:

☐ Email List

☐ user@example.com

☐ Enter Email Id

Start Date and time: IST

End Date and time: IST

☐ ☒ Schedule at a later time

4. (Optional) Select the **Do not save this report on Service Insight** check box if you do not want to save the PBN report. By default, the check box is clear and PBN reports are stored in the Service Insight database.
5. In the **Enter PBN Report Name** text box, enter a name for the PBN report.

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

6. For the **Create PBN Report for** option, select one of the following:
 - Select **All devices** if you want the PBN report to be generated for all the devices
 - Select **Selected devices shown below** if you want the PBN reports to be generated for only the selected devices in the page and select the devices listed below.
7. For the **Send Email To:** option, enter the e-mail address of the user to whom the PBN report must be sent.

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

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



NOTE:

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

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

The report generated for the first time has the name you provide. All successive reports have the date and time the report is generated appended to the name that you provide.

11. Click **Submit**.

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

12. 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.

13. If you want to cancel the job scheduled 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 305](#)

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 PNBs** page displays the list of PBNs that are associated with the device that you selected.

**Related
Documentation**

- [Exposure Analyzer Overview on page 294](#)
- [Targeted PBNs Overview on page 309](#)
- [Notifications Overview on page 314](#)

Managing EOL Reports

- [Managing EOL Reports on page 300](#)

Managing EOL Reports

- [EOL Reports Overview on page 300](#)
- [Exporting EOL Reports on page 302](#)
- [Deleting EOL Reports on page 303](#)
- [Regenerating EOL Reports on page 304](#)

EOL Reports Overview

The **EOL Reports** page displays the End of Life (EOL) reports that you generate as shown in [Figure 92 on page 301](#). 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 number in the **Devices Selected** field.

Figure 92: 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 36 on page 301 describes the fields on the **EOL Reports** page and the **EOL Report Detail** dialog box.

Table 36: 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 regenerated.
Created by	Name of the user who created the EOL report.
Devices selected	<p>Number of devices that were selected to generate the EOL report.</p> <p>Clicking the number takes you to the Exposure Analyzer page which displays only the devices with EOL parts.</p>
Devices with EOL parts	<p>Number of devices with parts for which end-of-life is announced or is in the process of being announced.</p> <p>The EOL date of a part specifies the date when Juniper Networks announced the end-of-life of the part.</p>
End of Life Announce parts	Number of parts in the devices in the EOL report for which EOL dates are announced.
End of Sale parts	<p>Number of parts in the devices in the EOL report for which the end of sale date has exceeded. Juniper Networks or a Juniper Networks partner do not sell these parts after the end of sale date.</p> <p>The end of sale date of a part specifies the last day to buy a product, order a new service contract, or add the part to an existing support contract. After the end of sale date, parts and services are removed from price lists.</p>
Last Hardware Engineering Support parts	<p>Number of parts in the devices in the EOL report for which hardware is no longer available for order or RMA.</p> <p>The last hardware engineering support date for a part specifies the last day the hardware engineering in Juniper Networks will support the part.</p>

Table 36: EOL Reports Page and EOL Report Detail Dialog Box Fields Description (*continued*)

Field	Description
Last Software Engineering Support parts	<p>Number of parts in the devices in the EOL report for which software or firmware is no longer available from Juniper Networks.</p> <p>The last software engineering support date of a part specifies the last date till which new (that is, non-maintenance) software releases will support the product. After this date, new software releases will not support the product. Maintenance releases of the major software releases issued prior to this date will support the product within the current software EOL guidelines.</p>
End of Service parts	<p>Number of parts in the devices in the EOL report for which end of service date is exceeded.</p> <p>The end of service date of a part specifies the last date to receive contracted service (including hardware and software bug fixes, and logistics replacement or repair services) for the part.</p>

You can perform the following tasks using the **EOL Reports** page:

- [Exporting EOL Reports on page 302](#)
- [Regenerating EOL Reports on page 304](#)
- [Deleting EOL Reports on page 303](#)

Related Documentation

[Generating EOL Reports on page 296](#)

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 the following information:

- **Product:** The device with parts for which EOL is announced.
- **Serial#:** Serial number of the device chassis. with parts for which EOL is announced.
- **Device:** The host name of the device.
- **PSN#:** The product specification notification for the part
- **EOL Model#:** The model number of the part for which EOL is announced.
- **Top Level Assembly#:** The top level assembly part number of the part for which EOL is announced.
- **Circuit Assembly Part#:** The circuit assembly part number of the part for which EOL is announced.
- **EOL Announce Date:** The date when Juniper Networks announced the end of life of a product
- **End of Sale Date:** The end of sale date of a part specifies the last day to buy a product, order a new service contract, or add the part to an existing support contract. After the end of sale date, parts and services are removed from price lists.
- **Last Software Engineering Date:** The last software engineering support date of a part specifies the last date till which new (that is, non-maintenance) software releases will

support the product. After this date, new software releases will not support the product. Maintenance releases of the major software releases issued prior to this date will support the product within the current software EOL guidelines.

- **Last Hardware Engineering Date:** The last hardware engineering support date for a part specifies the last day the hardware engineering in Juniper Networks will support the part.
- **End of Service Date:** The end of service date of a part specifies the last date to receive contracted service (including hardware and software bug fixes, and logistics replacement or repair services) for the part.
- **Replacement#:** The model number of the part with which the EOL part existing in the device can be replaced.

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 296](#)
- [EOL Reports Overview on page 300](#)

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 296](#)
- [EOL Reports Overview on page 300](#)

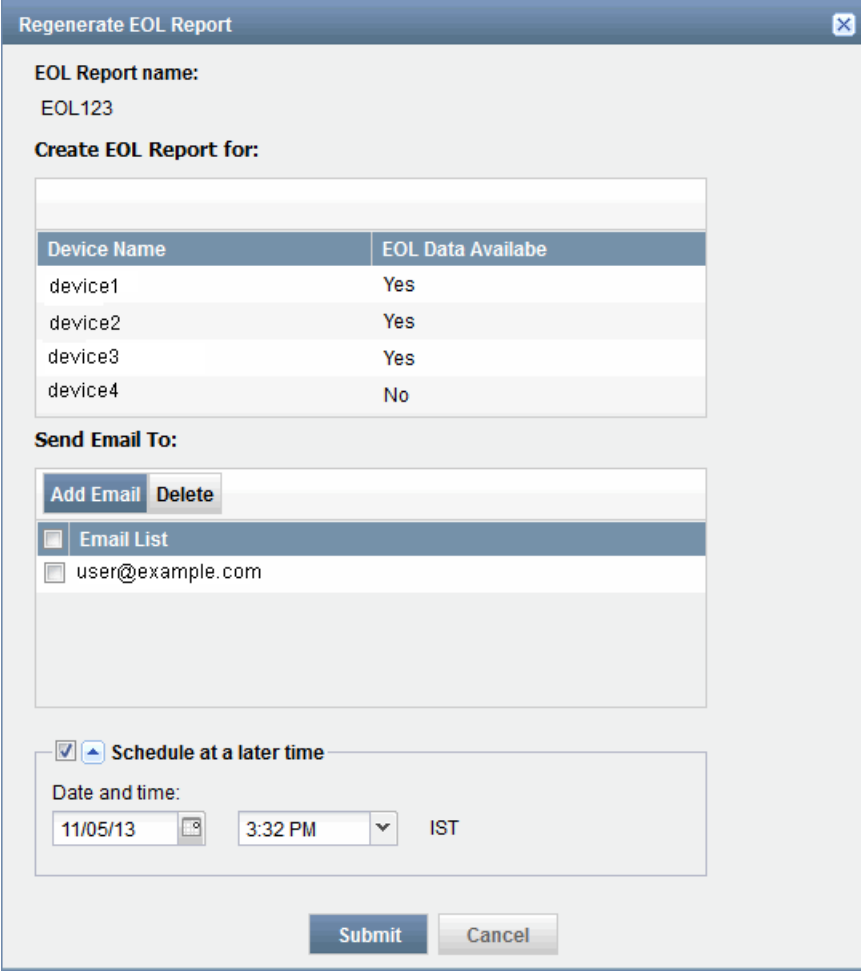
Regenerating EOL Reports

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 93 on page 304](#).

Figure 93: Regenerate EOL Report Dialog Box



The dialog box titled "Regenerate EOL Report" contains the following sections:

- EOL Report name:** EOL123
- Create EOL Report for:** A table with 2 columns: Device Name and EOL Data Available.

Device Name	EOL Data Available
device1	Yes
device2	Yes
device3	Yes
device4	No
- Send Email To:** Includes "Add Email" and "Delete" buttons, an "Email List" header, and a list containing "user@example.com".
- Schedule at a later time:** A checkbox is checked. Below it, "Date and time:" shows "11/05/13" (with a calendar icon), "3:32 PM" (with a dropdown arrow), and "IST".
- At the bottom are "Submit" and "Cancel" buttons.

4. (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.

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 EOL 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 **Jobs** page.

Related Documentation

- [Generating EOL Reports on page 296](#)
- [EOL Reports Overview on page 300](#)

Managing PBN Reports

- [PBN Reports Overview on page 305](#)
- [Exporting PBN Reports on page 306](#)
- [Deleting PBN Reports on page 306](#)
- [Regenerating PBN Reports on page 307](#)

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 94 on page 305](#).

Figure 94: 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 37 on page 305](#) describes the fields on the Manage PBN Reports page and the PBN Report Detail dialog box.

Table 37: 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.

Table 37: PBN Reports Page and PBN Report Detail Dialog Box Fields Description (*continued*)

Field	Description
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 306](#)
- [Regenerating PBN Reports on page 307](#)
- [Deleting PBN Reports on page 306](#)

**Related
Documentation**

- [Generating PBN Reports on page 297](#)

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 297](#)
- [PBN Reports Overview on page 305](#)

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 297](#)
 - [PBN Reports Overview on page 305](#)

Regenerating PBN Reports

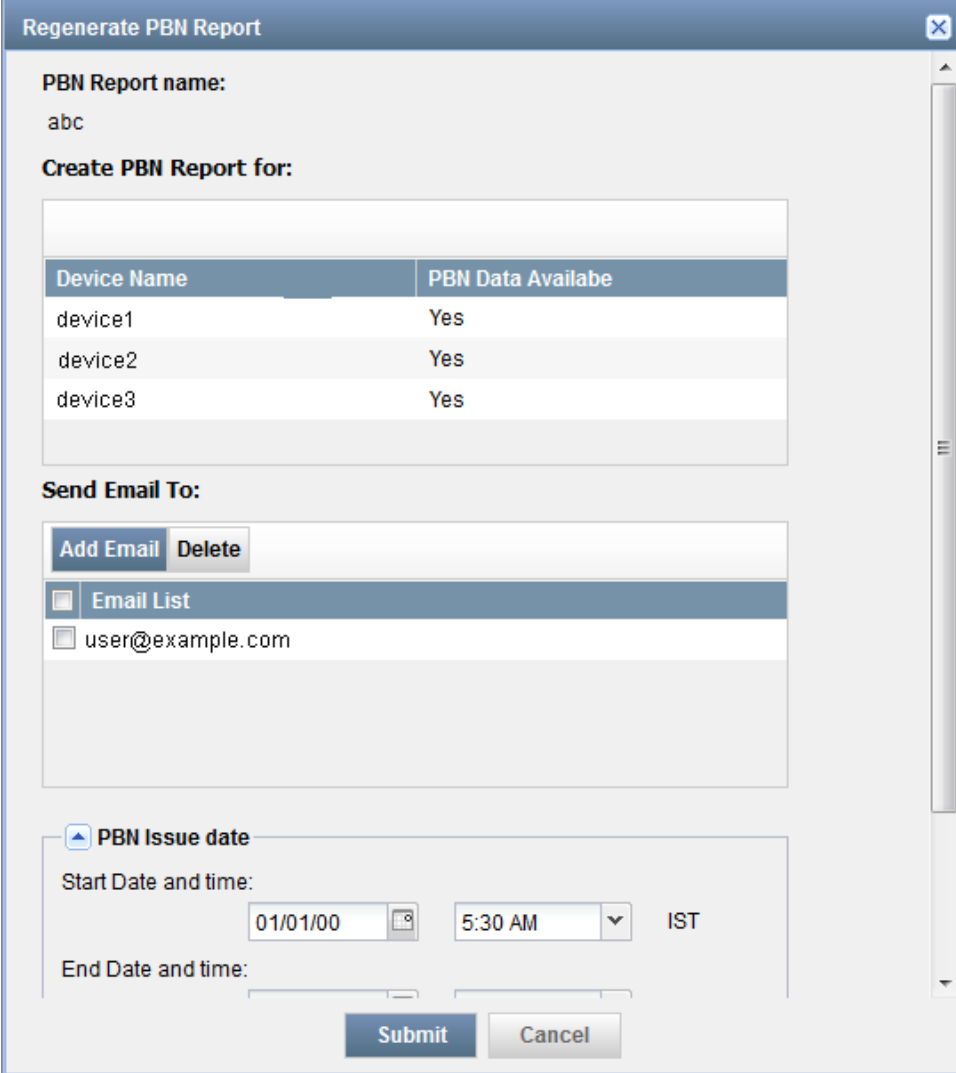
Junos Space Service Insight provides the *Regenerate PBN Reports* option on the Actions menu to regenerate reports on proactive bug notifications (PBNs) to get information about devices impacted by latest PBNs issued by Juniper Support System (JSS).

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. From the **Actions** menu, select **Regenerate PBN Reports**. Alternatively, right-click the PBN report and select **Regenerate PBN Reports**.

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 95 on page 308](#).

Figure 95: Regenerate PBN Report Dialog Box



The dialog box is titled "Regenerate PBN Report". It contains the following sections:

- PBN Report name:** A text field with the value "abc".
- Create PBN Report for:** A table with two columns: "Device Name" and "PBN Data Available".
- Send Email To:** A section with "Add Email" and "Delete" buttons, an "Email List" header, and a list containing "user@example.com".
- PBN Issue date:** A section with "Start Date and time" and "End Date and time" labels. The start date is "01/01/00" and the start time is "5:30 AM" with a dropdown arrow. The time zone is "IST". The end date and time fields are empty.
- At the bottom are "Submit" and "Cancel" buttons.

Device Name	PBN Data Available
device1	Yes
device2	Yes
device3	Yes

- (Optional) To add or delete users who must receive the e-mail, use the **Add Email** and **Delete** buttons respectively.
- (Optional) Under the **PBN issue date** option, select values for **Start Data and time** and **End Date and time** to generate a report of the devices affected by PBNs issued during the selected time period.

**NOTE:**

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

6. (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.
7. Click **Submit**.
The Job Information dialog box displays a *Job ID* link. Click this link to view the status of the job on the **Manage Jobs** page.

Related Documentation

- [Generating PBN Reports on page 297](#)
- [PBN Reports Overview on page 305](#)

Managing PBNs

- [Managing PBNs on page 309](#)

Managing PBNs

- [Targeted PBNs Overview on page 309](#)
- [Scanning PBNs for Impact on Devices on page 311](#)
- [Flagging PBNs to Users on page 311](#)
- [Assigning an Owner to a PBN on page 312](#)
- [Deleting PBNs on page 312](#)
- [E-Mailing PBNs on page 313](#)

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 38 on page 310](#) describes the fields displayed on the **Manage PBNs** page and the PBNs detail summary view.

Table 38: 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 294](#)
 - [Scanning PBNs for Impact on Devices on page 311](#)

- [Assigning an Owner to a PBN on page 312](#)
- [Flagging PBNs to Users on page 311](#)
- [E-Mailing PBNs on page 313](#)

Scanning PBNs for Impact on Devices

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 294](#)
- [Assigning an Owner to a PBN on page 312](#)

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 294](#)
- [Scanning PBNs for Impact on Devices on page 311](#)
- [Assigning an Owner to a PBN on page 312](#)

Assigning an Owner to a PBN

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 294](#)
- [Scanning PBNs for Impact on Devices on page 311](#)

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 294](#)
 - [Scanning PBNs for Impact on Devices on page 311](#)
 - [Assigning an Owner to a PBN on page 312](#)

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 294](#)
 - [Scanning PBNs for Impact on Devices on page 311](#)
 - [Assigning an Owner to a PBN on page 312](#)

Managing Notifications

- [Managing Notifications on page 313](#)

Managing Notifications

- [Notifications Overview on page 314](#)
- [Creating and Copying a Notification on page 315](#)
- [Editing the Filters and Actions of a Notification on page 317](#)
- [Enabling and Disabling Notifications on page 317](#)
- [Deleting Notifications on page 318](#)

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 39 on page 314](#) provides more information about the fields on the **Manage Notifications** page.

Table 39: 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 309](#)
 - [Creating and Copying a Notification on page 315](#)
 - [Enabling and Disabling Notifications on page 317](#)

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 315](#)
- [Copying a Notification on page 315](#)

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 40 on page 316](#).
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 40 on page 316](#).
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 40: Manage Notifications Page Field Description

Field	Description	Range/Length
Name	Enter the name of the notification.	64 characters
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 309](#)
- [Enabling and Disabling Notifications on page 317](#)

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 309](#)
- [Creating and Copying a Notification on page 315](#)
- [Enabling and Disabling Notifications on page 317](#)

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 309](#)
 - [Creating and Copying a Notification on page 315](#)

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 309](#)
 - [Creating and Copying a Notification on page 315](#)
 - [Enabling and Disabling Notifications on page 317](#)

CHAPTER 12

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.

PAR-3000

System Log Message Get Intel Update Failed

Description Failed to get Intelligence update from Service Now partner.

Type Error

Action Contact Juniper Networks Partner.

PAR-3001

System Log Message Case submission failed

Description Failed to submit the case to Service Now partner.

Type Error

Action Contact Juniper Networks Partner.

PAR-3002

System Log Message Case dampened in the Partner Proxy

Description The Service Now partner is not allowing a case to be created for an incident.

Type Error

Action Contact Juniper Networks Partner.

PAR-3003

System Log Message IJMB upload failed

Description IJMB could not be uploaded to the Service Now partner.

Type Error

Action Contact Juniper Networks Partner.

PAR-3004

System Log Message Case update failed

Description The status of a case could not be updated in the Service Now partner.

Type Error

Action Contact Juniper Networks Partner.

PAR-3005

System Log Message Partner Proxy does not accept BIOS incidents

Description The Service Now partner does not allow cases to be created for BIOS incidents.

Type Error

Action Contact Juniper Networks Partner.

PAR-3006

System Log Message Partner Proxy does not accept AIS Health Check incidents

Description The Service Now partner does not allow cases to be created for AI-Scripts Health Check incidents.

Type Error

Action Contact Juniper Networks Partner.

PAR-3007

System Log Message Partner Service Now Is not reachable

Description The Service Now partner is down and cannot be reached.

Type Error

Action Contact Juniper Networks Partner.

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 335](#)

Index

A

AI-Script	
install.....	114
remove.....	117
AI-Scripts	
downloading i3ninstall packages.....	37
install location on device hard disk.....	39
install package versioning.....	38

B

BIOS data	
collect.....	145

C

collect	
BIOS data.....	145
RSI output.....	124
system log.....	124
conventions	
notice icons.....	xvii
copying a notification.....	315
creating a notification.....	315
customer support.....	xviii
contacting JTAC.....	xviii

D

dashboard overview	
Dashboard Gadgets.....	64
Service Now Workspaces.....	63
deleting	
device.....	131
device group.....	107
iJMB.....	268
incident.....	239
information message.....	261
notification policy.....	281
organization.....	101
device	
add, service now.....	114
associate with device group.....	132

device group	
create.....	105
modify.....	107
disabling a notification.....	317
documentation	
comments on.....	xviii

E

enabling a notification.....	317
EOL reports	
deleting.....	303
exporting.....	302
overview.....	300
regenerating.....	304
export device data	
CSV/Excel.....	119
export iJMB	
html.....	265
export inventory information	
CSV/Excel.....	119
exposure analyzer overview.....	294

G

generating	
on-demand iJMBs, off-box.....	266
on-demand iJMBS, on-box.....	266
on-demand incidents, off-box.....	121
on-demand incidents, on-box.....	121
generating eol reports.....	296
generating pbn reports.....	297
global settings	
global.....	202
proxy server.....	207
snmp server	
add	204
edit/delete.....	206

I

incident	
assigning owner.....	234
export to Excel.....	237
flagging.....	235
submitting.....	239
information message	
assign connected member.....	262
assign owner.....	260
flagging.....	261
insight central overview.....	293

J

JMB error.....	270
----------------	-----

M

managing SNMP Traps.....	207
manuals	
comments on.....	xviii
modes	
Service Now.....	59

N

notice icons.....	xvii
notification policy	
create.....	274
enable/disable.....	281
notifications	
deleting.....	318
editing filters and actions.....	317
overview.....	314

O

organization	
add.....	95
modify.....	100
run in test mode.....	103
test connection to JSS.....	102
overview	
administration.....	91
AI-Scripts.....	27
device groups.....	105, 108
device snapshots.....	264
EOL reports.....	300
exposure analyzer	294
Incidents.....	232
insight central.....	293
messages.....	259
notifications.....	272, 314
organization.....	93
Service Automation.....	21
Service Central	229
service insight.....	285
service insight dashboard.....	286
targeted PBNs.....	309

P

PBN reports	
deleting.....	306
regenerating.....	307

PBNs

deleting.....	312
e-mailing.....	313
flagging to users.....	311
overview.....	309
scanning for impact.....	311
show matching PBNs.....	300

S

script bundle	
add.....	200
delete.....	201
Service Automation	
overview.....	21
service insight	
dashboard gadgets.....	287
dashboard overview.....	286
overview.....	285
user roles.....	291
Service Now	
modes.....	59
service now	
add, device.....	114
Service Now Overview.....	48
support, technical See technical support	

T

technical support	
contacting JTAC.....	xviii

U

user roles.....	69
service insight.....	291

V

view	
case in Case Manager.....	254
incident details	244
JMB details.....	268
viewing exposure.....	120