



AI-Scripts, Service Now, and Service Insight

User Guide

Release

18.1R1



Modified: 2018-12-13

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

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

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

Service Automation User Guide

Release 18.1R1

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

Revision History

22 December, 2018—AI-Scripts Release 7.0R2.0, Service Now and Service Insight Release 18.1R1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xix
	Documentation and Release Notes	xix
	Documentation Conventions	xix
	Documentation Feedback	xx
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxi
Chapter 1	Automated Support And Prevention Overview	23
	Automated Support and Prevention Overview	23
	Benefits of ASAP	25
	Juniper Networks Devices Supported by Service Now and Service Insight	25
Part 1	AI-Scripts	
Chapter 2	AI-Scripts Overview	35
	AI-Scripts Overview	35
	Working Modes of AI-Scripts	35
	Events Detected by AI-Scripts	36
	Types of JMBs	36
	JMB Contents	37
	Logs	43
	Installing AI-Scripts	44
	Downloading AI-Scripts Install Packages and Release Notes	45
	AI-Scripts Install Package Versioning	45
	AI-Scripts Install Locations on Devices	46
	Automatically Installing AI-Scripts Bundles	46
	Manually Installing AI-Scripts on Devices	46

Part 2	Junos Space Service Now	
Chapter 3	Service Now Overview	53
	Junos Space Service Now Overview	54
	Junos Space Service Now Overview	54
	Benefits of Junos Space Service Now	55
	Service Now Domain Overview	56
	Assigning a Service Now Object to Another Domain	58
	Installing, Upgrading, and Uninstalling Junos Space Service Now and Junos	
	Space Service Insight Applications	58
	Uploading a Service Now Image File to Junos Space server	59
	Installing Junos Space Service Now and Junos Space Service Insight	60
	Upgrading Junos Space Service Now and Junos Space Service Insight	62
	Uninstalling Junos Space Service Now and Junos Space Service Insight	63
	Service Now MIBs	64
	Service Now MIBs	64
	Service Now Modes	64
	Junos Space Service Now Modes	65
	Service Now Dashboard and Workspaces Overview	68
	Service Now Dashboard Overview	69
	Service Now Workspaces	69
	Dashboard Gadgets	69
	Service Now Inventory Pages	71
	Filtering Inventory Pages on Service Now and Service Insight	71
	User Roles	74
	Junos Space Service Now User Roles	74
Chapter 4	Using the Service Now Getting Started Assistant	79
	Service Now Getting Started Assistant Usage Overview	79
	Service Now Getting Started Assistant Usage Overview	79
Chapter 5	Trouble Ticket APIs Supported by Service Now	81
	Trouble Ticket APIs Overview	81
	Profiles Used by Service Now	82
	Setting up Java Based Web Service Client	82
	Accessing a Web Service	88
	Trouble Ticket APIs Supported by Service Now	89
	Error Messages Displayed by OSS/J Client	90
	Trouble Ticket Attributes Supported by Service Now	92
	Trouble Ticket Events Supported by Service Now	94

Chapter 6	Administration	97
	Service Now Administration Workspace Overview	97
	Organizations	98
	Service Now Organizations Overview	99
	Associated Actions	101
	Creating Organizations	101
	Adding an Organization to Service Now	102
	Adding an End Customer to Service Now Configured in Partner Proxy Mode	104
	Modifying Organization Parameters	107
	Deleting an Organization	107
	Testing the Connection to JSS	108
	Viewing Messages Assigned to an End Customer	109
	Running an Organization in Test Mode	110
	Updating Core File Upload Configuration for an End Customer	110
	Device Groups	111
	Service Now Device Groups Overview	111
	Associated Actions	112
	Creating a Device Group	112
	Modifying a Device Group	114
	Deleting a Device Group	115
	Service Now Devices	116
	Service Now Devices Overview	117
	Associated Actions	122
	Adding Devices to Junos Space Service Now	123
	Installing an Event Profile on a Device by Using Service Now	124
	Uninstalling an Event Profile from a Device	128
	Exporting Device Data in CSV and Excel Formats	130
	Exporting Inventory Information in CSV Format	131
	Viewing Exposure for a Device	132
	Generating an On-Demand Incident	133
	Collecting RSI and System Log Files	138
	Generating an RMA Incident for a Device	142
	Moving a Device to Maintenance Mode	145
	Deleting a Device from Junos Space Service Now	147
	Associating Devices with a Device Group	148
	Assigning an Auto Submit Policy to a Device	148
	Configuring AI-Scripts Parameters by Using Junos Space Service Now	150
	Viewing Incidents Created for a Device	152
	Verifying the Connection Between a Device and the SFTP Server	153
	Service Now End Customer–Partner Communication Overview	153
	Generating CSR by Service Now Partner	154
	Obtaining Signature of a Certificate Authority	157
	Uploading the Certificate to Service Now Partner	157
	Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate	157
	Obtaining SSL Certificate of the Service Now Partner	157
	Installing the SSL Certificate on a Service Now End Customer	158

BIOS Validation	160
Service Now BIOS Validation Overview	160
Associated Actions	162
Configuring BIOS Validation for Verifying BIOS Integrity of a Device	162
Event Profiles and AI-Scripts	164
Service Now Event Profiles Overview	165
Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview	166
Associated Actions	169
Adding an Event Profile to Junos Space Service Now	170
Cloning an Event Profile	174
Importing Event Profiles into Junos Space Service Now in XML Format	178
Exporting Event Profiles from Junos Space Service Now in XML Format	180
Deleting Event Profiles from Junos Space Service Now	182
Viewing an Event Profile	182
Pushing an Event Profile to Devices	183
Displaying Devices Associated with an Event Profile	186
Setting an Event Profile as the Default Event Profile in Junos Space Service Now	187
Exporting Events Data in Excel Format	188
Adding a Script Bundle to Junos Space Service Now	188
Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now	189
Deleting a Script Bundle from Junos Space Service Now	190
Global Settings	191
Configuring Global Settings	191
Adding an SNMP Configuration to Service Now	194
Editing an SNMP Configuration	196
Managing SNMP Traps	196
Viewing Proxy Server Settings Configured on the Junos Space Platform	197
Configuring SFTP Server for Uploading Core Files Generated for Events	198
Directive File Overview	200
Viewing the Directive File	201
Updating the Directive File in Junos Space Service Now	202
Restoring the Default Directive File	204
Configuring Advanced Filter Settings	205
Incident Filters	207
Service Now Incident Filters Overview	207
Associated Actions	208
Viewing Incident Filters Configured on Junos Space Service Now	209
Creating Incident Filters	210
Creating a Basic Incident Filter	210
Creating an Advanced Incident Filter	212
Importing Incident Filters to Service Now	213
Modifying an Incident Filter	214
Deleting Incident Filters	216
Exporting Incident Filters	218
Reordering Incident Filters	219
Enabling Incident Filters	220

Disabling Incident Filters	221
Auto Submit Filters	222
Service Now Auto Submit Filters Overview	222
Actions That You Can Perform From the Auto Submit Filters Task	224
Viewing Auto Submit Filters	225
Creating Auto Submit Filters	226
Creating a Basic Auto Submit Filter	226
Creating an Advanced Auto Submit Filter	228
Importing Auto Submit Filters to Service Now	230
Modifying an Auto Submit Filter	230
Exporting Auto Submit Filters	233
Reordering Auto Submit Filters	234
Enabling Auto Submit Filters	236
Disabling Auto Submit Filters	237
Assigning an Auto Submit Filter to a Domain	238
Deleting Auto Submit Filters	239
Auto Submit Policy	240
Service Now Auto Submit Policy Overview	241
Associated Actions	242
Creating an Auto Submit Policy	243
Modifying an Auto Submit Policy	248
Deleting Auto Submit Policies from Service Now	249
Exporting an Incidents Report	250
Changing the Status of Auto Submit Policies	251
Changing the Dampening Status of an Auto Submit Policy	253
Product Health Data Collection	254
Service Now Product Health Data Collection Overview	254
Viewing Product Health Data Files Collected from a Device	256
Product Health Data Collection Configuration Overview	259
Benefits of Product Health Data Collection	261
Actions That You Can Perform From the Product Health Data Collection Task	261
Configuring Product Health Data Collection on a Device	262
Configuring PHDC by Using the Product Health Data Collection Task	262
Configuring PHDC by Using the Service Now Devices Task	264
Modifying a Product Health Data Collection Configuration	267
Rescheduling a Product Health Data Collection Configuration	270
Retrying Collecting Product Health Data from a Device	271
Disabling Product Health Data Collection on a Device	273
Enabling Product Health Data Collection on a Device	274
Aborting a Product Health Data Collection Configuration	275
Exporting Product Health Data Information to an Excel File	276
Exporting Information about Devices on which PHDC is configured	277
Exporting Data about PHD Files Collected from a Device	279
Deleting Product Health Data Files Collected from a Device	281
Deleting a Product Health Data Collection Configuration from Service Now	283

	Address Groups	284
	Service Now Address Group Overview	285
	Associated Actions	285
	Creating an Address Group	286
	Modifying an Address Group	286
	Deleting Address Groups	287
	Associating Devices with an Address Group From the Address Groups Page	287
	Associating Devices with an Address Group From the Organizations Page	289
	Associating Devices with an Address Group from the Device Groups Page	290
	Associating Devices with an Address Group from the Service Now Devices Page	292
	E-mail Templates	292
	Service Now E-Mail Templates Overview	293
	Associated Actions	295
	Viewing E-Mail Templates	296
	Modifying an E-Mail Template	297
Chapter 7	Service Central	299
	Service Central Overview	299
	Incidents	301
	Service Now Incidents Overview	302
	Associated Actions	304
	Assigning an Owner to an Incident	305
	Flagging an Incident to a User	306
	Checking Incident Status Updates	307
	Exporting a Juniper Message Bundle (JMB) to an HTML file	308
	Deleting an Incident	310
	Submitting an Incident to Juniper Support Systems or Service Now Partner	311
	Viewing Incident Details	316
	Viewing Knowledge Base Articles Associated with an Incident	319
	Uploading an Attachment to an Incident	320
	Updating an End-Customer Case	322
	Uploading Core Files to JSS for an Incident	323
	Associating an Incident with an Existing Case	324
	Technical and End Customer Support Cases	326
	Service Now Technical Support Cases and End Customer Support Cases Overview	326
	Associated Actions	329
	Viewing a Case in Case Manager	330
	Uploading an Attachment to a Case	331

Collecting Additional Information for Incidents and Cases	333
Collecting Additional Information for Service Now Incidents and Cases	
Overview	334
Associated Actions	334
Viewing Junos OS Commands Configured for Collecting Additional	
Information About an Incident	335
Configuring Junos OS Commands to Collect Additional Information About	
an Incident	336
Modifying the Settings for Collecting Additional Information for an	
Incident	339
Deleting the Settings for Collecting Additional Information for an	
Incident	341
Downloading the Additional Information Collected About an Incident	342
Viewing Junos OS Commands Configured for Collecting Additional	
Information for a Technical Support Case	344
Configuring Junos OS Commands to Collect Additional Information for a	
Technical Support Case	345
Modifying the Configuration for Collecting Additional Information for a	
Technical Support Case	348
Downloading the Additional Information Collected for a Technical Support	
Case	350
Deleting the Configuration for Collecting Additional Information for a	
Technical Support Case	351
Information	352
Service Now Messages Overview	353
Associated Actions	353
Assigning Ownership to Messages	353
Flagging a Message to Users	354
Deleting a Message	355
Assigning a Message to an End Customer	355
Service Now Device Snapshots Overview	357
Associated Actions	358
Exporting Device Snapshots to HTML	358
Generating an On-Demand Device Snapshot	359
Deleting Device Snapshots	361
Viewing Details of a Device Snapshot	362
Device Analysis	363
Viewing BIOS Validations	363
Exporting BIOS Validation Results	366
Deleting BIOS Validation Incidents	367
Viewing Product Health Data Files Collected from a Device	368
Exporting Product Health Data Information to an Excel File	371
Exporting Information about Devices on which PHDC is configured . . .	372
Exporting Data about PHD Files Collected from a Device	374
Deleting Product Health Data Files Collected from a Device	376
JMB Errors	378
JMBs with Errors	378
Downloading JMBs with Errors	379
Deleting JMBs with Errors	380

	Suppressed Events	380
	Service Now Suppressed Events Overview	380
	Associated Actions	381
	Deleting JMBs for Suppressed Events	381
	Viewing Details of JMBs for Suppressed Events	382
	Creating Incidents for Suppressed Juniper Message Bundles	383
	Notifications	384
	Service Now Notification Policies Overview	384
	Associated Actions	386
	Creating and Editing a Notification Policy	386
	Enabling or Disabling a Notification Policy	395
	Deleting a Notification Policy	395
Part 3	Junos Space Service Insight	
Chapter 8	Introduction to Service Insight	399
	Service Insight Overview	399
	Service Insight Overview	399
	Service Insight Dashboard	401
	Dashboard Gadgets	401
	Service Insight Workspaces	403
	Benefits of Junos Space Service Insight	403
	Service Insight Domain Overview	403
	Assigning a Service Insight Object to Another Domain	404
Chapter 9	User Roles	407
	Junos Space Service Insight User Roles	407
Chapter 10	Insight Central	409
	Insight Central Overview	409
	Insight Central Overview	409
	Insight Central Overview	409
	Exposure Analyzer	410
	Exposure Analyzer	410
	Exposure Analyzer Overview	410
	Generating EOL Reports	413
	Generating PBN Reports	415
	Viewing PBNs for a Device	419
	Managing EOL Reports	419
	Managing EOL Reports	419
	Service Insight EOL Reports Overview	420
	Exporting EOL Reports	421
	Deleting EOL Reports	423
	Regenerating EOL Reports	423
	Managing PBN Reports	425
	Service Insight PBN Reports Overview	425
	Associated Actions	426
	Exporting PBN Reports	426
	Deleting PBN Reports	427
	Regenerating PBN Reports	427

	Managing PBNs	429
	Managing PBNs	429
	Service Insight Targeted PBNs Overview	430
	Scanning PBNs for Impact on Devices	432
	Flagging PBNs to Users	432
	Assigning an Owner to a PBN	433
	Deleting PBNs	434
	E-Mailing PBNs	434
	Managing Notifications	435
	Managing Notifications	435
	Service Insight Notifications Overview	435
	Creating and Copying a Notification	436
	Editing the Filters and Actions of a Notification	439
	Enabling and Disabling Notifications	439
	Deleting Notifications	440
Chapter 11	JSS Messages Reference	441
	LIC-1001	441
	LIC-1098	441
	LIC-1099	442
	LIC-2000	442
	LIC-2099	442
	LIC-3000	442
	LIC-4000	442
	LIC-4001	443
	LIC-4002	443
	LIC-4003	443
	LIC-4004	443
	LIC-4005	444
	LIC-4006	444
	LIC-4007	444
	LIC-4008	444
	LIC-4009	445
	LIC-4010	445
	LIC-4011	445
	PAR-3000	445
	PAR-3001	446
	PAR-3002	446
	PAR-3003	446
	PAR-3004	446
	PAR-3005	447
	PAR-3006	447
	PAR-3007	447
	PVS-1000	447
	PVS-1001	447
	PVS-1002	448
	PVS-1006	448
	PVS-1007	448
	PVS-1008	448

	PVS-1009	449
	PVS-1010	449
	PVS-1011	449
	PVS-1100	449
	PVS-1200	449
	PVS-1201	450
	PVS-1202	450
	PVS-1203	450
	PVS-1204	450
	PVS-1205	451
	PVS-1207	451
	PVS-1210	451
	PVS-1213	451
	PVS-1214	451
	PVS-1215	452
	PVS-1216	452
	PVS-1223	452
	PVS-1226	452
	PVS-1227	453
	PVS-1230	453
	PVS-1231	453
	PVS-1232	453
	PVS-8000	453
	PVS-8001	454
	PVS-8002	454
	PVS-8006	454
	PVS-9000	454
	PVS-9999	454
	SEC-1000	455
	SEV-0001	455
	SEV-0002	455
	SEV-0003	455
	VLD-1000	455
	VLD-2000	456
Chapter 12	Appendix	457
	Sample Perl Script for Incident and Auto Submit Filters	457

List of Figures

Part 1	AI-Scripts	
Chapter 2	AI-Scripts Overview	35
	Figure 1: Attachment Section of a JMB	43
	Figure 2: Log Section of a JMB	44
Part 2	Junos Space Service Now	
Chapter 3	Service Now Overview	53
	Figure 3: Service Now Operating in Direct Mode	66
	Figure 4: Service Now Operating in Partner Proxy and End Customer Modes	67
	Figure 5: Platform with Most Incidents Gadget	70
	Figure 6: Devices with Most Incidents Gadget	71
Chapter 6	Administration	97
	Figure 7: Organizations Page	99
	Figure 8: Add Organization Dialog Box	102
	Figure 9: Add Member Dialog Box	105
	Figure 10: Test Connection Dialog Box	109
	Figure 11: Messages Assigned to Connected Member Page	109
	Figure 12: Core File Upload Configuration Page	111
	Figure 13: Create Device Group Page	113
	Figure 14: Associate Case ID Dialog Box	114
	Figure 15: Select Devices to Add to Service Now and Click Submit Page	124
	Figure 16: Install Event Profile Page	125
	Figure 17: Uninstall Event Profiles Dialog Box	129
	Figure 18: On-demand Incident Dialog Box	135
	Figure 19: Create On-demand Incident Status Dialog Box	138
	Figure 20: Configure File Collections Dialog Box	140
	Figure 21: Request RMA page	143
	Figure 22: Configure Maintenance Mode Dialog Box	146
	Figure 23: Modify Auto Submit Policy Page	149
	Figure 24: Advanced Parameters Settings for AI-Scripts	151
	Figure 25: Service Now Partner Communicating with a Service Now End Customer and JSS Using SSL Certificate	154
	Figure 26: BIOS Validation Legal Notice on Service Now Partner	161
	Figure 27: BIOS Validation Legal Notice on Service Now End Customer	162
	Figure 28: Configure BIOS Validation Dialog Box	163
	Figure 29: View Event Profiles Page	166
	Figure 30: Install Event Profile Page	168
	Figure 31: Uninstall Event Profile Dialog Box	169

Figure 32: Add Event Profile Page	171
Figure 33: Potential Exposure to Known Issues Page	173
Figure 34: View Event Profiles Page	179
Figure 35: Export All Data Dialog Box	181
Figure 36: Export All Data Dialog Box	181
Figure 37: Push to Devices Dialog Box	184
Figure 38: Potential Exposure to Known Issues Page	185
Figure 39: View Event Profiles Page	187
Figure 40: Add Script Bundle Dialog Box	189
Figure 41: Global Settings Page	192
Figure 42: SNMP Trap Attribute Page	197
Figure 43: Core File Upload Configuration Page	199
Figure 44: Directive File Page	200
Figure 45: Directive File Page	201
Figure 46: Directive File Dialog Box	203
Figure 47: Directive File Upload Dialog Box	204
Figure 48: Advanced Settings Page	205
Figure 49: Incident Filters Page	209
Figure 50: Create Basic Filter Page for Creating Basic Incident Filters	211
Figure 51: Create Advanced Filter Page for Creating Advanced Incident Filters	213
Figure 52: Import Incident Filters Dialog Box	214
Figure 53: Modify Basic Filter Page for Modifying a Basic Incident Filter	215
Figure 54: Delete Incident Filters Dialog Box	217
Figure 55: Export Incident Filters Dialog Box	218
Figure 56: Re-order Filters page for Reordering Incident Filters	219
Figure 57: Enable Incident Filters Dialog Box	220
Figure 58: Disable incident Filters Dialog Box	221
Figure 59: Auto Submit Filters Page	223
Figure 60: Auto Submit Filters Page	225
Figure 61: Create Basic Filter for Creating a Basic Auto Submit Filter	227
Figure 62: Create Advanced Filter Page for Creating an Advanced Filter	229
Figure 63: Import Auto Submit Dialog Box	230
Figure 64: Modify Advanced Filter Page for Modifying an Advanced Auto Submit Filter	231
Figure 65: Export Auto Submit Filters Dialog Box	234
Figure 66: Re-order Filters Dialog Box for Reordering Auto Submit Filters	235
Figure 67: Enable Auto Submit Filters Dialog Box	236
Figure 68: Disable Auto Submit Filters Dialog Box	237
Figure 69: Assign Auto Submit Filters to Domain Dialog Box	238
Figure 70: Delete Auto Submit Filters Dialog Box	240
Figure 71: Auto Submit Policy Page	241
Figure 72: Auto Submit Policy Creation Page	243
Figure 73: Choose events to include in Auto Submit Policy Page	244
Figure 74: Change Auto Submit Policy Status Page	252
Figure 75: Change Auto Submit Policy Dampening Status Page	253
Figure 76: Product Health Data Devices Page	255
Figure 77: View All Product Health Data Files Page	256
Figure 78: View All Devices of this PHDC Page	258
Figure 79: Product Health Data Collection Page	260

	Figure 80: Configure PHDC Page	262
	Figure 81: Configure Product Health Data Collection	263
	Figure 82: Configure Product Health Data Collection Dialog Box	265
	Figure 83: Modify Product Health Data Collection Page	269
	Figure 84: Modify Product Health Data Collection Parameters	269
	Figure 85: Retry on Failed Devices Page	272
	Figure 86: Disable Collection on Devices Page	273
	Figure 87: Enable Collection on Devices Page	274
	Figure 88: Abort Product Health Data Collection Dialog Box	276
	Figure 89: PHDC Information of Devices Exported to Excel	277
	Figure 90: PHD Files Information Exported to Excel	277
	Figure 91: View all Devices of this PHDC	278
	Figure 92: View All Product Health Data Files Page	280
	Figure 93: View All Devices of this PHDC Page	280
	Figure 94: View All Product Health Data Files Page	282
	Figure 95: View All Devices of this PHDC Page	282
	Figure 96: View all Product Health Data Files Page	284
	Figure 97: Associate Address Group to Devices Page	288
	Figure 98: Associate Devices to Address Group Page	290
	Figure 99: Associate Devices to Address Group Page	291
	Figure 100: E-Mail Templates Page	293
	Figure 101: Email Templates Page	296
Chapter 7	Service Central	299
	Figure 102: Service Central Gadgets	300
	Figure 103: Export JMB to HTML Dialog Box	309
	Figure 104: Submit Case Options Page	312
	Figure 105: Incident Detail Page	318
	Figure 106: Upload Attachment Dialog Box	321
	Figure 107: End-Customer Cases Dialog Box	322
	Figure 108: Associate Case ID Page	325
	Figure 109: View Tech Support Cases	327
	Figure 110: View End Customer Cases Page	328
	Figure 111: Upload Attachment Dialog Box	332
	Figure 112: Collect Additional Information Jobs Results Summary page	336
	Figure 113: Collect Additional Information Page	337
	Figure 114: Modify Collect Additional Information page	340
	Figure 115: Cancel Job Dialog Box	342
	Figure 116: Collect Additional Information Attachment Details Tab on the Incident Details Page	343
	Figure 117: Collect Additional Information Jobs Results Summary Page	344
	Figure 118: Collect Additional Information Page	347
	Figure 119: Modify Collect Additional Information Page	349
	Figure 120: Cancel Job Dialog Box	352
	Figure 121: Choose Connected Members Dialog Box	356
	Figure 122: On-demand Incident Dialog Box	360
	Figure 123: Juniper Message Bundle	362
	Figure 124: View JMB Dialog Box	363
	Figure 125: View All Product Health Data Files Page	368

Figure 126: View All Devices of this PHDC Page	370
Figure 127: PHDC Information of Devices Exported to Excel	371
Figure 128: PHD Files Information Exported to Excel	372
Figure 129: View all Devices of this PHDC	373
Figure 130: View All Product Health Data Files Page	375
Figure 131: View All Devices of this PHDC Page	375
Figure 132: View All Product Health Data Files Page	377
Figure 133: View All Devices of this PHDC Page	377
Figure 134: Download JMB Errors Dialog Box	379
Figure 135: Suppressed Events Page	381
Figure 136: Delete Suppressed Events Dialog Box	382
Figure 137: Create Incident for Suppressed JMBs Dialog Box	384
Figure 138: Create Notifications Page	387

Part 3

Chapter 10

Junos Space Service Insight

Insight Central	409
Figure 139: Insight Central Landing Page	410
Figure 140: Exposure Analyzer Page	412
Figure 141: Generate PBN Report Dialog Box	417
Figure 142: EOL Reports Page View	420
Figure 143: Regenerate EOL Report Dialog Box	424
Figure 144: PBN Reports page	425
Figure 145: Regenerate PBN Report Dialog Box	428
Figure 146: Targeted PBNs Page	430

List of Tables

	About the Documentation	xix
	Table 1: Notice Icons	xx
Chapter 1	Automated Support And Prevention Overview	23
	Table 2: Devices Supported by Junos Space Service Now	26
Part 1	AI-Scripts	
Chapter 2	AI-Scripts Overview	35
	Table 3: Elements in the Manifest Section of a JMB	37
Part 2	Junos Space Service Now	
Chapter 3	Service Now Overview	53
	Table 4: Service Now Objects and Their Default Domains	57
	Table 5: Features and Tasks Enabled for Service Now Modes	67
	Table 6: Filter-enabled Tables and Columns	72
	Table 7: Predefined Roles for the Service Now Application	75
Chapter 5	Trouble Ticket APIs Supported by Service Now	81
	Table 8: Trouble Ticket APIs Supported by Service Now	89
	Table 9: OSS/J Client Error Scenarios	90
	Table 10: Supported Trouble Ticket Attributes	93
Chapter 6	Administration	97
	Table 11: Organization Column Descriptions	100
	Table 12: Description of Fields on the Add Organization Page	103
	Table 13: Device Group Parameters	112
	Table 14: Service Now Devices Field Descriptions	117
	Table 15: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs	136
	Table 16: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs	143
	Table 17: Event Profile Parameters	166
	Table 18: Add Event Profile Page Field Descriptions	171
	Table 19: Global Settings Parameters	192
	Table 20: Fields in Incident Filters Page	209
	Table 21: Fields on Auto Submit Filters Page	223
	Table 22: Fields on Auto Submit Filters Page	225
	Table 23: Auto Submit Policy Parameters	241
	Table 24: Icons That Represent the Event Types and Their Descriptions	245
	Table 25: Fields on the Product Health Data Devices Page	255

	Table 26: Fields on the View All Product Health Data Files Page	257
	Table 27: Fields on the Product Health Data Collection Page	260
	Table 28: List of E-Mail Templates Provided by Service Now and the Modes in which the Templates can be Used	294
Chapter 7	Service Central	299
	Table 29: Fields on the Incidents Page	302
	Table 30: Fields on the View Tech Support Cases Page	327
	Table 31: Fields on the View End Customer Cases Page	329
	Table 32: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs	360
	Table 33: BIOS Validations Field Descriptions	364
	Table 34: BIOS Validation Field Descriptions	366
	Table 35: Fields on the View All Product Health Data Files Page	368
	Table 36: Notification Triggers and Trigger Filters	385
	Table 37: Create Notification Policy Page Field Descriptions	389
Part 3	Junos Space Service Insight	
Chapter 8	Introduction to Service Insight	399
	Table 38: Service Insight Objects and Their Default Domains	404
Chapter 9	User Roles	407
	Table 39: Predefined Roles for the Service Insight Application	407
Chapter 10	Insight Central	409
	Table 40: Exposure Analyzer Page Icon Descriptions	412
	Table 41: Device Details from the Exposure Analyzer Page	412
	Table 42: EOL Reports Page and EOL Report Detail Dialog Box Fields Description	420
	Table 43: PBN Reports Page and PBN Report Detail Dialog Box Fields Description	425
	Table 44: Targeted PBNs Field Descriptions	430
	Table 45: Description of Fields on Notifications Page	436
	Table 46: Notifications Page Field Description	438

About the Documentation

- Documentation and Release Notes on page xix
- Documentation Conventions on page xix
- Documentation Feedback on page xx
- Requesting Technical Support on page xxi

Documentation and Release Notes

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







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

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

Documentation Conventions

Table 1 on page xx defines notice icons used in this documentation.

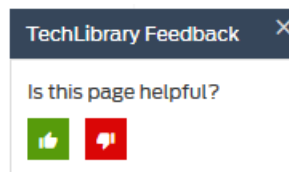
Table 1: Notice Icons

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



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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active 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 <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

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 <https://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 <https://www.juniper.net/support/requesting-support.html>.

CHAPTER 1

Automated Support And Prevention Overview

- [Automated Support and Prevention Overview on page 23](#)
- [Juniper Networks Devices Supported by Service Now and Service Insight on page 25](#)

Automated Support and Prevention Overview

Juniper Networks Automated Support And Prevention (ASAP) is an end-to-end solution designed to automatically resolve product issues, prevent outages, provide insight and increase network productivity. With ASAP, a network operator can perform the following functions:

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

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

- Advanced Insight-Scripts (AI-Scripts):

AI-Scripts are XML, XSLT, or SLAX scripts installed on devices running Junos OS Release 11.4 or later to detect hardware and software events such as fan failure, read-write errors, routing protocol checksum error, critical packet drops, and failure to commit configurations. When an event occurs on a device on which AI-Scripts are installed, AI-Scripts are triggered to collect troubleshooting information from the device, which is bundled in a structured format called a Juniper Message Bundle (JMB).

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

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

- Junos Space Service Now and Junos Space Service Insight applications:

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

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

For more information about the directive file, see [“Directive File Overview” on page 200](#)

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

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

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

- Juniper Support Systems (JSS):

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

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

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

- Juniper Case Analysis Tool Suite (JCATS)

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

Benefits of ASAP

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

Related Documentation

- [AI-Scripts Overview on page 35](#)
- [Service Now Overview on page 54](#)
- [Service Insight Overview on page 399](#)
- *Installing Junos Space Service Now and Junos Space Service Insight Applications*

Juniper Networks Devices Supported by Service Now and Service Insight

[Table 2 on page 26](#) lists all the Juniper Networks product series and devices supported by Junos Space Service Now Release 18.1R1 and AI-Scripts Release 7.0R4. For information about devices supported by Junos Space Network Management Platform, see [Devices Supported by Junos Space Network Management Platform](#).

Table 2: Devices Supported by Junos Space Service Now

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

Table 2: Devices Supported by Junos Space Service Now (continued)

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

Table 2: Devices Supported by Junos Space Service Now (continued)

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

Table 2: Devices Supported by Junos Space Service Now (continued)

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

Table 2: Devices Supported by Junos Space Service Now (continued)

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

Table 2: Devices Supported by Junos Space Service Now (continued)

Product Series	Devices
SRX Series	SRX100
	SRX110H-VB
	SRX210
	SRX220
	SRX240
	SRX300
	SRX320
	SRX320-PoE
	SRX340
	SRX345
	SRX550
	SRX550-M
	SRX650
	SRX1400
	SRX1500
	SRX3400
	SRX3600
	SRX4100
	SRX4200
	SRX5400, SRX5600, SRX5800
Virtual SRX Series	Firefly Perimeter, vSRX NOTE: vSRX devices running Junos OS release earlier than Junos OS 15.1x are called Firefly Perimeter.
T Series	T320
	T640
	T1600
	T4000
	TX Matrix
	TX Matrix Plus
	TXP-3D

Table 2: Devices Supported by Junos Space Service Now (continued)

Product Series	Devices
Virtual MX Series	vMX
Virtual route reflector (VRR)	VRR

- Related Documentation
- [Adding Devices to Junos Space Service Now on page 123](#)
 - *Installing AI-Scripts on a Device*

PART 1

AI-Scripts

- [AI-Scripts Overview on page 35](#)

CHAPTER 2

AI-Scripts Overview

- [AI-Scripts Overview on page 35](#)
- [Installing AI-Scripts on page 44](#)

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.

An AI-Scripts bundle contains event policies. An event policy defines the Junos OS commands that are executed to collect troubleshooting data when an event occurs on the device. One event policy is defined for each event. For information about adding a script bundle to Service Now, see [“Adding a Script Bundle to Junos Space Service Now” on page 188](#).

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 events, 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 generates data about the event, packages the data in a structured format called a Juniper Message Bundle (JMB), and stores the JMB at a defined location on the device from where Junos Space Service Now accesses the data.

This section contains the following topics:

- [Working Modes of AI-Scripts on page 35](#)
- [Events Detected by AI-Scripts on page 36](#)
- [Types of JMBs on page 36](#)
- [JMB Contents on page 37](#)
- [Logs on page 43](#)

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. The on-demand JMBs can be of two types—on-box on-demand JMB or off-box on-demand JMB.

An on-box on-demand JMB is generated by AI-Scripts installed on the device in response to on-demand request by user. An off-box on-demand JMB is generated by Service Now by executing preconfigured commands on the device. You can use the off-box on-demand JMB to get information about a device when AI-Scripts are not installed on the device.

Events Detected by AI-Scripts

AI-Scripts detect the following types of events:

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

For a complete list of events detected by AI-Scripts:

- for AI-Scripts Releases earlier than 6.0R1.0, refer to the latest version of *AI-Scripts Release Notes* at [Service Automation Index Page](#)
- for AI-Scripts Releases 6.0R1.0 and later, refer to the *AI-Scripts Feature Guide* at [AI-Scripts 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.

Starting in Service Now Release 15.1R1, the Manifest section displays the following information: RSI Collection, BIOS Validation, Log Collection, Junos Software Version, Junos Space Version, Service Now Version, Product Health Data Collection, Product Health Data Collection Command File, JMB Cleanup Interval.

[Table 3 on page 37](#) lists the elements present in a JMB manifest.

Table 3: Elements in the Manifest Section of a JMB

Element	Description
Event Information	

Table 3: Elements in the Manifest Section of a JMB (continued)

Element	Description
Host Event-ID	<p>Specifies the ID of the event in response to which the JMB is generated</p> <p>Host Event-ID is represented in the following format:</p> <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 3: 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 3: 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 3: 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 3: 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.

Starting in Service Now Release 15.1R2, the Attachments section displays the statuses of reading each attachment from the device and uploading each attachment file to JSS or Service Now partner.

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 1 on page 43 shows the Attachment section of a JMB.

Figure 1: 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 2 on page 44 shows the log section of a JMB.

Figure 2: Log Section of a JMB

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

Release History Table

Release	Description
15.1R2	Starting in Service Now Release 15.1R2, the Attachments section displays the statuses of reading each attachment from the device and uploading each attachment file to JSS or Service Now partner.
15.1R1	Starting in Service Now Release 15.1R1, the Manifest section displays the following information: RSI Collection, BIOS Validation, Log Collection, Junos Software Version, Junos Space Version, Service Now Version, Product Health Data Collection, Product Health Data Collection Command File, JMB Cleanup Interval

Related Documentation

- [Adding a Script Bundle to Junos Space Service Now on page 188](#)
- [Deleting a Script Bundle from Junos Space Service Now on page 190](#)

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 188](#).
- 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 46](#).

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* at [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 45](#)
- [AI-Scripts Install Package Versioning on page 45](#)
- [AI-Scripts Install Locations on Devices on page 46](#)

- [Automatically Installing AI-Scripts Bundles on page 46](#)
- [Manually Installing AI-Scripts on Devices on page 46](#)

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 at the [AI-Scripts](#) download site. Also, download the *Advanced Insight Scripts (AI-Scripts) Release Notes*.

Before you begin, ensure that you have an account and a valid service contract with Juniper Networks. If you do not have an account, complete the registration form at <https://www.juniper.net/registration/Register.jsp> to open an account.

To download an AI-Scripts install package:

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

<https://www.juniper.net/support/downloads/?p=serviceautomation>.

2. Log in to the Juniper Networks authentication system using the username and password provided by Juniper Networks.
3. Download the AI-Scripts install package.

If you want to install 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 to copy the file to the device while installing AI-Scripts on the device..

To install AI-Scripts automatically on a group of devices, download the 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 releases prior to AI-Scripts Release 6.0R1.0
jais-m.nZx.x-signed.tar for AI-Scripts Release 6.0R1.0 and later
```

For example:

```
jais-5.0R1.0-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 latest [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 use Junos Space Service Now to install an AI-Scripts bundle on devices. For information about using Service Now to install AI-Scripts bundles, see [“Adding a Script Bundle to Junos Space Service Now”](#) on page 188.

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



NOTE: We recommend that you always use Service Now for installing AI-Scripts Release 5.0 and later on devices running Junos OS.

Manually Installing AI-Scripts on Devices

AI-Scripts Releases prior to 5.0R2.0 can be installed on Junos OS devices manually by 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 Network Management Platform.



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

To install AI-Scripts Release 4.XRX or earlier manually on a device:

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.

AI-Scripts is installed on the device if AI-Scripts [version] is displayed in the output of 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 install AI-Scripts 5.0 (5.0R2, 5.0R3, and 5.0R4) and later releases manually on a device:



BEST PRACTICE: We recommend you to use Service Now to install AI-Scripts Release 5.0R2.0 and later. For information about installing AI-Scripts Release 5.0R2.0 and later on a device by using Service Now, see [“Installing an Event Profile on a Device by Using Service Now” on page 124](#).



NOTE:

- AI-Scripts Release 5.0R2.0 or later cannot be installed on QFabric devices.
- You cannot install AI-Scripts Release 6.0R1 and later on a device manually. Service Now displays a warning message on the Service Now GUI when AI-Scripts Release 6.0R1 and later is manually installed on a device.

1. Copy the AI-Scripts install package (example: jais-5.0R2.0-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 device and is stored on the device by Service Now while installing AI-Scripts.

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.

See Also • [Adding a Script Bundle to Junos Space Service Now on page 188](#)

PART 2

Junos Space Service Now

- [Service Now Overview on page 53](#)
- [Using the Service Now Getting Started Assistant on page 79](#)
- [Trouble Ticket APIs Supported by Service Now on page 81](#)
- [Administration on page 97](#)
- [Service Central on page 299](#)

CHAPTER 3

Service Now Overview

- [Junos Space Service Now Overview on page 54](#)
- [Installing, Upgrading, and Uninstalling Junos Space Service Now and Junos Space Service Insight Applications on page 58](#)
- [Service Now MIBs on page 64](#)
- [Service Now Modes on page 64](#)
- [Service Now Dashboard and Workspaces Overview on page 68](#)
- [Service Now Inventory Pages on page 71](#)
- [User Roles on page 74](#)

Junos Space Service Now Overview

- [Junos Space Service Now Overview on page 54](#)
- [Service Now Domain Overview on page 56](#)

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. Your contract with Juniper Networks determines whether Service Now operates in direct 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 [“Junos Space Service Now Modes” on page 65](#).

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 detects the event and automatically collects diagnostic data and packages the data in an XML file called *Juniper Message Bundle (JMB)*.

For information about AI-Scripts, see [“AI-Scripts Overview” on page 35](#).

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 policies (known as auto submit policies) to automatically submit an incident to JSS as soon as the incident is created. Service Now provides options to define the level of information that you share in a JMB 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.
- View device snapshots, BIOS data, and product health data.

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 device snapshots to JSS. 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 group the devices into device groups and 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 manage groups of devices with similar attributes or uses efficiently.

Service Now also sends SNMP traps if notification policies are configured to send traps when events occur on devices. From Service Now and Service Insight Release 14.1R1, 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 69](#).

From Release 14.1R1 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 Now Getting Started 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 Platform and other Junos Space applications are still running. Refer to [“Junos Space Service Now User Roles” on page 74](#) for information about tasks that can be performed for a user role.

Benefits of Junos Space Service Now

- **Automatic collection of troubleshooting information**—Information, such as system logs, core files, request support information, and so on, required for troubleshooting an event is automatically collected by AI-Scripts and submitted to Service Now.
- **Automatic submission of incidents and troubleshooting information to JSS**—Auto submit policies configured on Service Now help you to submit the details of issues that occurred on a device and the associated troubleshooting information to JSS to create a case, significantly reducing time and effort to resolve the issue.

- **Ensure optimal health of managed devices**—Device snapshots, BIOS validations, and product health data collection features help you proactively identify potential risks with your devices and mitigate any network downtime due to the risks.

- See Also**
- [Service Now Administration Workspace Overview on page 97](#)
 - [Service Automation Implementation Guide](#)

Service Now 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 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 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 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 in the system domain and objects such as organization, script bundle, SNMP configuration, and Email template, which are assigned to the domain that you are currently in, are visible to you. If you are assigned to more than one domain, you can access the other domains and objects in those domains by selecting the domains from the **Login as username** in list present on the Service Now banner. 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 58](#).

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 end customer.

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 4 on page 57](#) lists Service Now objects and their default domains.

Table 4: 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 • Auto Submit Filter • Incident Filter 	Domain to which a user is logged in	Global domain
<ul style="list-style-type: none"> • Global Setting • Directive File • SNMP Configuration • Core File Upload Configuration • Message • Script Bundle • Email Template • End Customer Information Message • Script Installation Advisor (SIA) 	System domain	System domain
<ul style="list-style-type: none"> • Service Now Device • Incident • Device Snapshot • Error JMB • Technical Support Case • End Customer Case 	Domain assigned to the device in Junos Space Network Management Platform	Domain assigned to the device in Junos Space Network Management Platform

Assigning a Service Now Object to Another Domain

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

To assign a Service Now object to another domain:

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

The object's page appears.

2. On the Object's 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 to which you want to assign the object 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 on the service Now banner, 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.

- See Also**
- [Service Central Overview on page 299](#)
 - [Service Now Administration Workspace Overview on page 97](#)
 - [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 59](#)
- [Installing Junos Space Service Now and Junos Space Service Insight on page 60](#)
- [Upgrading Junos Space Service Now and Junos Space Service Insight on page 62](#)
- [Uninstalling Junos Space Service Now and Junos Space Service Insight on page 63](#)

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 <https://www.juniper.net/support/downloads/?p=servicenow> 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 <https://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, see [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 59](#) 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 18.1 is listed, select **Service Now Release 18.1** and then click **Install**.
- If Service Now Release 18.1 is not listed, upload the Service Now Release 18.1 image file to the Junos Space server.

To upload the a Service Now image file to the Junos Space server, see [“Uploading a Service Now Image File to Junos Space server” on page 59](#).

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 to Service Now Release 18.1R1 and Service Insight Release 18.1R1 from Service Now Release 17.2R1 and Service Insight Release 17.2R1.

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 <https://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 59 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 GUI 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 59](#).

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**.
Verify that 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.

See Also • [AI-Scripts Overview on page 35](#)

- [Service Now Overview on page 53](#)
- [Service Insight Overview on page 399](#)

Service Now MIBs

- [Service Now MIBs on page 64](#)

Service Now MIBs

Service Now supports Juniper Networks enterprise-specific management information bases (MIBs). These MIBs define the traps that Service Now sends to the SNMP server you configure on Service Now. The traps correspond to the trigger defined for notification policies. For information about notification policies, see “[Service Now Notification Policies Overview](#)” on page 384.

Using Service Now notifications, you can configure Service Now to send SNMP traps to one or more configured 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 the MIB files:

1. From the list to select Junos Space applications on the Junos Space GUI, select **Service Now**.

The dashboard appears, which displays the **Service Now Notices** box.

2. 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 page provides links to the Service Now MIBs for different Service Now releases.

3. Click a Service Now version to download the respective MIB file.

- See Also**
- [Adding an SNMP Configuration to Service Now on page 194](#)
 - [Junos Space Service Now Overview on page 54](#)
 - [Service Now MIBs Downloads](#)

Service Now Modes

- [Junos Space Service Now Modes on page 65](#)

Junos Space Service Now Modes

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

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

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

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

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

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

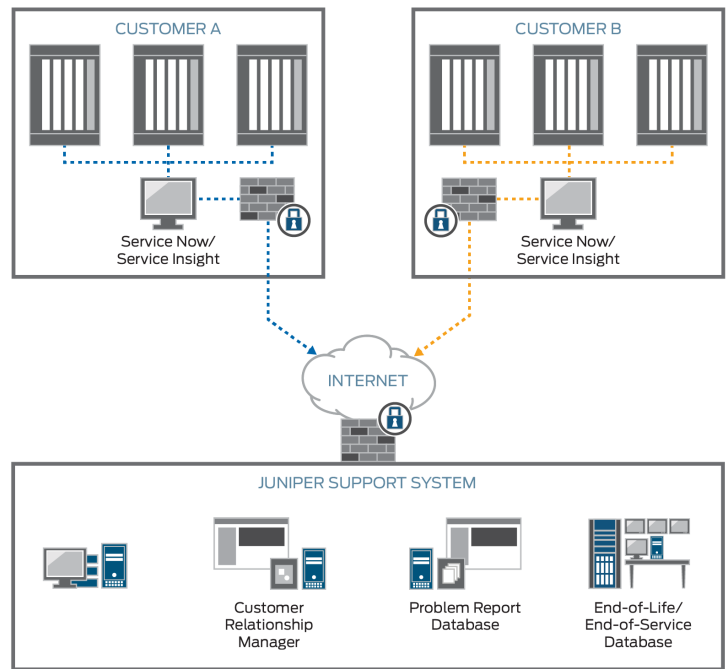


NOTE: If Service Now is already in End Customer mode, you cannot operate it in Offline mode.

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

Figure 3 on page 66 shows Service Now operating in Direct mode.

Figure 3: Service Now Operating in Direct Mode



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

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

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

You can configure only one organization, but can manage multiple devices in this mode. [Figure 4 on page 67](#) shows Service Now operating in Partner Proxy and End Customer modes.

Figure 4: Service Now Operating in Partner Proxy and End Customer Modes

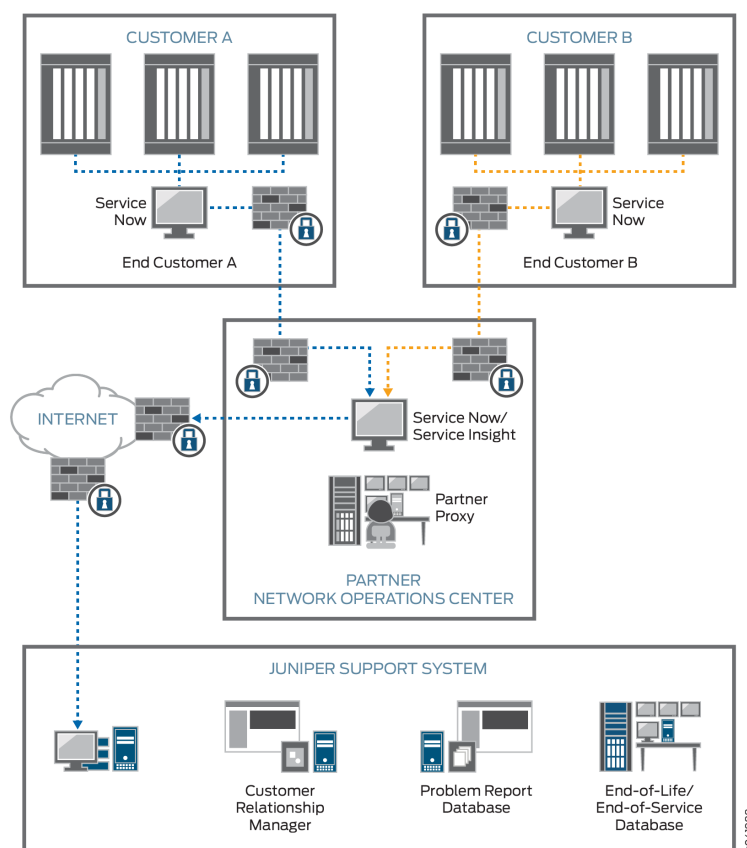


Table 5 on page 67 highlights some of the differences among the various modes of operating Service Now.

Table 5: 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 5: 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

- See Also**
- [Service Now Administration Workspace Overview on page 97](#)
 - [Service Central Overview on page 299](#)
 - [Configuring Global Settings on page 191](#)
 - [Adding an Organization to Service Now on page 102](#)
 - [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 104](#)

Service Now Dashboard and Workspaces Overview

- [Service Now Dashboard Overview on page 69](#)

Service Now Dashboard Overview

The Service Now dashboard displays notifications and graphs about platforms and devices with most incidents. Dashboard is the default page that appears on the Service Now GUI when you access the Service Now application.

The Service Now dashboard includes:

- [Service Now Workspaces on page 69](#)
- [Dashboard Gadgets on page 69](#)

Service Now Workspaces

Apart from the Service Central and Administration workspaces, Service Now also provides shortcuts to the Devices and Jobs workspaces of Junos Space Network Management Platform by including them in the Service Now navigation tree.

For more details about devices and jobs workspace, refer to [Workspaces Feature Guide](#).

You can perform the following tasks by using the Service Central workspaces:

- View and manage incidents
- View and manage technical support cases
- (only in Partner Proxy mode) View and manage end-customer cases
- View and manage informative messages from Juniper Support System (JSS) or Service Now partner (in End Customer mode)
- View and manage device snapshots
- View and manage BIOS validations and product health data
- View and manage JMB with errors
- View and manage JMBs for which incidents are not created
- Configure and manage notification policies for informing users about events that occurred on devices.

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:

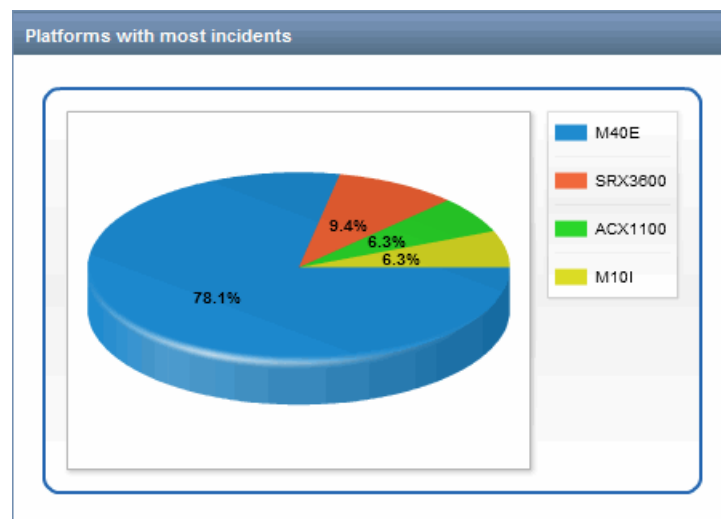
- [Platforms with Most Incidents on page 70](#)
- [Devices with the Most Incidents on page 70](#)
- [Service Now Notices \(Upgrade and Contract Notice\) on page 71](#)

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 5 on page 70](#)), the Incidents page displays only those incidents that are detected on the ACX1100 router.

Figure 5: Platform with Most Incidents Gadget



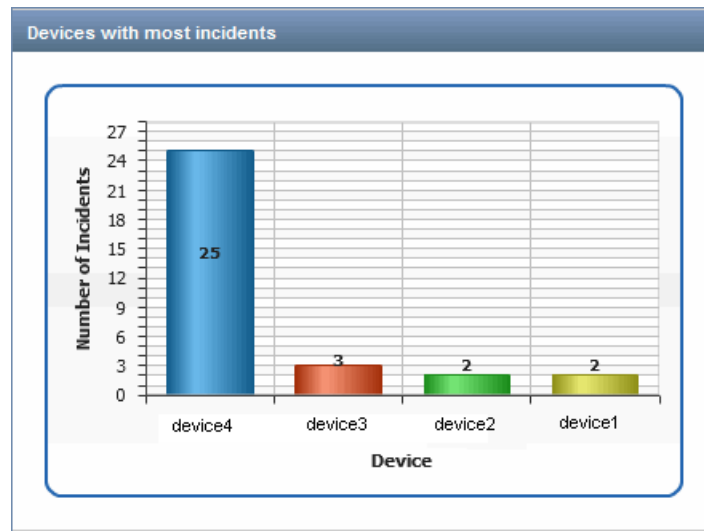
Devices with the Most Incidents

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.

By using the Devices with Most Incidents gadget, you can also filter all incidents created for a device on the Incidents page. To do this, click the **Devices** bar of your choice in the graph to take you to the Incidents page, which displays only those incidents that affect the device that you selected.

As shown in [Figure 6 on page 71](#), 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 6: 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.

- See Also**
- [Service Central Overview on page 299](#)
 - [Service Now Administration Workspace Overview on page 97](#)

Service Now Inventory Pages

- [Filtering Inventory Pages on Service Now and Service Insight on page 71](#)

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 72](#) 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
	Incident Filter	All columns except: <ul style="list-style-type: none"> • Attributes
	Auto Submit Filter	All columns except: <ul style="list-style-type: none"> • Attributes
	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
	Suppressed Events	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*.

- See Also**
- [Service Central Workspace Overview on page 299](#)
 - [Service Insight Workspaces on page 403](#)

User Roles

- [Junos Space Service Now User Roles on page 74](#)

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 75](#) 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"> • Incident Filters: Create basic filter, create advanced filter, import incident filters, modify incident filters, delete incident filters, export incident filters, reorder incident filters, enable incident filters, disable incident filters, and assign incident filters to a domain • Auto Submit Filters: Create basic filter, create advanced filter, import auto submit filters, modify auto submit filters, delete auto submit filters, export auto submit filters, reorder auto submit filters, enable auto submit filters, disable auto submit filters, and assign auto submit filters to a domain • Global Settings: Manage directive file, configure an FTP server for uploading core files, manage SNMP traps, and configure Service Now partner certificates on a Service Now end customer, configure advanced settings • Address Group: Create address groups, associate address groups with devices, modify address groups, delete address groups, and assign address groups to domains • Device Groups: Create device groups, modify device groups, set a device group as the default device group, associate address groups with device groups, assign device groups to domains, and delete device groups from Service Now • Service Now Devices: Add devices to Service Now, export device inventory information, associate devices with autosubmit policies, associate devices with device groups, check FTP server configuration, configure RSI and log file collection on devices, create on-demand incidents, associate devices with address groups, export device information, install event profiles on devices, request Return Materials Authorisation (RMA), uninstall event profile from devices, view exposure of devices to known events, view incidents generated on Service Now, assign the Service Now devices to domains, and delete devices from Service Now • Email Templates: Modify default content of an Email template and restore the modified content of an Email template to its default content • Event Profiles: Add AI-Scripts bundles to Service Now, set an AI-Scripts bundle as the default AI-Scripts bundle in Service Now, delete AI-Script bundles, create event profiles, import event profiles, export event profiles to an XML file, push event profiles to devices, clone event profiles, set an event profile as the default profile, view events included in event profiles, view devices associated with event profiles, assign event profiles to domains, and delete event profiles from Service Now • Auto Submit Policy: Create autosubmit policies, export incident reports, modify autosubmit policies, change the dampening status of autosubmit policies, assign autosubmit policies to a domain, and delete autosubmit policies from Service Now • Organization: Add an organization to Service Now, add end customers to 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 • Suppressed Events: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • Notifications: Create notifications, edit notification filters and actions, copy notifications, delete notifications, enable or disable notifications, and assign notifications to domains
Service Now Read Only	Administration	Service Now Devices: Export event profiles, export devices, view exposure of devices to known events, and create on-demand device snapshots, export information about product health data and devices, download product health data files
	Service Central	<ul style="list-style-type: none"> • Incidents: Export a JMB in HTML format, view JMBs, export incident summary to Excel, and view tech support and end-customer cases in Case Manager • JMB Errors: Download error JMBs • Tech Support cases: View tech support cases in Case Manager and update cases • Information: View iJMBs, export iJMBs to HTML and scan devices for impact based on messages received from JSS • Device Analysis: Export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • Suppressed Events: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • Notifications: Create notifications • End-customer cases: View end-customer cases in Case Manager

Table 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 • Suppressed Events: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • View Tech Support Cases: View tech support cases in case manager, update cases in case manager • Information: Assign owners to messages received from JSS, flag messages received from JSS to users, delete messages received from JSS, assign messages received from JSS to end customers, export iJMBs to HTML, view iJMBs, and delete iJMBs from Service Now • Device Analysis: Delete BIOS validations, export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • View End Customer Cases: View end-customer cases in Case Manager and update end-customer cases • Notifications: Create notifications, edit filters and notifications, copy notifications, enable or disable notifications, assign notifications to domains, and delete notifications

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 User Accounts in Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide* available at

https://www.juniper.net/documentation/en_US/release-independent/junos-space/index.html.

- See Also**
- [Service Central Overview on page 299](#)
 - [Service Now Administration Workspace Overview on page 97](#)
 - [Junos Space Service Insight User Roles on page 407](#)

CHAPTER 4

Using the Service Now Getting Started Assistant

- [Service Now Getting Started Assistant Usage Overview on page 79](#)

Service Now Getting Started Assistant Usage Overview

- [Service Now Getting Started Assistant Usage Overview on page 79](#)

Service Now Getting Started Assistant Usage Overview

The Getting Started assistant is a section in the Junos Space help that guides you through the tasks that you can perform as part of the initial setup for every Junos Space 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 Junos Space 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 Service Now in Direct mode.

The Getting Started Assistant provides the following steps to start working with Service Now:

1. Review Global Settings.
See [“Configuring Global Settings” on page 191](#).
2. Create an Organization.
See [“Adding an Organization to Service Now” on page 102](#).
3. Add Devices to Junos Space.
See the *Discovering Devices* section of the [Workspaces Feature Guide](#).
4. Create a Device Group.

See [“Creating a Device Group”](#) on page 112.

5. Install Scripts using Service Now Devices.

See [“Installing an Event Profile on a Device by Using Service Now”](#) on page 124.

The following step is optional:

- Add a New Script Bundle.

See [“Adding a Script Bundle to Junos Space Service Now”](#) on page 188.

See Also • [Junos Space Service Now Overview](#) on page 54

CHAPTER 5

Trouble Ticket APIs Supported by Service Now

- [Trouble Ticket APIs Overview on page 81](#)
- [Profiles Used by Service Now on page 82](#)
- [Setting up Java Based Web Service Client on page 82](#)
- [Accessing a Web Service on page 88](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)

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 <https://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 54](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)
- [Setting up Java Based Web Service Client on page 82](#)

- [Profiles Used by Service Now on page 82](#)
- [Accessing a Web Service on page 88](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

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 54](#)
- [Trouble Ticket APIs Overview on page 81](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)
- [Setting up Java Based Web Service Client on page 82](#)
- [Accessing a Web Service on page 88](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

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.HttpsURLConnection;
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.wsd1.troubleticket.v1_2.JVTTroubleTicketSessionWSPort;
import org.ossj.wsd1.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 54](#)
- [Trouble Ticket APIs Overview on page 81](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)
- [Accessing a Web Service on page 88](#)
- [Profiles Used by Service Now on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

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 username 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 services 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 54](#)
- [Trouble Ticket APIs Overview on page 81](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)
- [Setting up Java Based Web Service Client on page 82](#)
- [Profiles Used by Service Now on page 82](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

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 by using the given key and returns only the requested attributes
getTroubleTicketsByKeys	Obtains multiple trouble tickets by using the given keys and returns only the requested attributes
setTroubleTicketByValue	Updates a single trouble ticket by 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 54](#)
- [Trouble Ticket APIs Overview on page 81](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)
- [Setting up Java Based Web Service Client on page 82](#)
- [Profiles Used by Service Now on page 82](#)
- [Accessing a Web Service on page 88](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

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 54](#)
 - [Trouble Ticket APIs Overview on page 81](#)
 - [Trouble Ticket APIs Supported by Service Now on page 89](#)
 - [Trouble Ticket Attributes Supported by Service Now on page 92](#)
 - [Trouble Ticket Events Supported by Service Now on page 94](#)
 - [Setting up Java Based Web Service Client on page 82](#)
 - [Accessing a Web Service on page 88](#)
 - [Profiles Used by Service Now on page 82](#)

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 54](#)
- [Trouble Ticket APIs Overview on page 81](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Trouble Ticket Events Supported by Service Now on page 94](#)
- [Setting up Java Based Web Service Client on page 82](#)
- [Profiles Used by Service Now on page 82](#)
- [Accessing a Web Service on page 88](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

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 92](#). 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 92](#). 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 54](#)
- [Trouble Ticket APIs Overview on page 81](#)
- [Trouble Ticket APIs Supported by Service Now on page 89](#)
- [Trouble Ticket Attributes Supported by Service Now on page 92](#)
- [Setting up Java Based Web Service Client on page 82](#)
- [Profiles Used by Service Now on page 82](#)
- [Accessing a Web Service on page 88](#)
- [Error Messages Displayed by OSS/J Client on page 90](#)

CHAPTER 6

Administration

- [Service Now Administration Workspace Overview on page 97](#)
- [Organizations on page 98](#)
- [Device Groups on page 111](#)
- [Service Now Devices on page 116](#)
- [BIOS Validation on page 160](#)
- [Event Profiles and AI-Scripts on page 164](#)
- [Global Settings on page 191](#)
- [Incident Filters on page 207](#)
- [Auto Submit Filters on page 222](#)
- [Auto Submit Policy on page 240](#)
- [Product Health Data Collection on page 254](#)
- [Address Groups on page 284](#)
- [E-mail Templates on page 292](#)

Service Now Administration Workspace Overview

Junos Space Service Now Administration workspace allows you to perform all administrative tasks such as configuring the operating mode of Service Now, adding devices discovered by Junos Space Network Management Platform, installing AI-Scripts on devices, configuring SNMP destinations for sending notifications, establishing connection with Juniper Support Systems, and so on. Only a user with Service Now Admin privileges can perform the tasks in the Administration workspace.

Administrative tasks that you can perform depend on the mode in which you configure Service Now to operate. See *Service Now Modes* for details.

The Administrative workspace dashboard graphically displays the number of devices in a device group and devices that are not sending snapshots.

You can perform the following tasks from the Administration workspace:

The Administration workspace enables you to perform the following tasks:

- Configure and manage organizations; see [“Service Now Organizations Overview” on page 99](#) for information about organization.
- Configure and manage device groups; see [“Service Now Device Groups Overview” on page 111](#) for information about device groups.
- Add devices discovered by Junos Space Platform and manage the devices; see [“Service Now Devices Overview” on page 117](#) for information about Service Now devices.
- Add AI-Scripts package to Service Now, configure event profiles using the AI-Scripts package and install event profiles on devices; see [“AI-Scripts Overview” on page 35](#) for information about AI-Scripts package and event profiles.
- Configure global settings for Service Now; see [Junos Space Service Now Global Settings Overview](#) for information about global settings.
- Configure and manage incident filters; see [“Service Now Incident Filters Overview” on page 207](#) for information about incident filters.
- Configure and auto submit filters; see [“Service Now Auto Submit Filters Overview” on page 222](#) for information about auto submit filters.
- Configure and manage auto submit policies; see [“Service Now Auto Submit Policy Overview” on page 241](#) for information about auto submit policies.
- Configure and manage product health data collection on devices; see [“Service Now Product Health Data Collection Overview” on page 254](#) for information about product health data collection.
- Configure address groups; see [“Service Now Address Group Overview” on page 285](#) for information about address groups.
- Manage e-mail templates; see [“Service Now E-Mail Templates Overview” on page 293](#) for information about e-mail templates.

**Related
Documentation**

- [Junos Space Service Now Overview on page 54](#)
- [Service Insight Overview on page 399](#)

Organizations

- [Service Now Organizations Overview on page 99](#)
- [Creating Organizations on page 101](#)
- [Modifying Organization Parameters on page 107](#)
- [Deleting an Organization on page 107](#)
- [Testing the Connection to JSS on page 108](#)
- [Viewing Messages Assigned to an End Customer on page 109](#)
- [Running an Organization in Test Mode on page 110](#)
- [Updating Core File Upload Configuration for an End Customer on page 110](#)

Service Now Organizations Overview

An organization in Junos Space Service Now represents a unique site ID in the Customer Relationship Manager (CRM) of the 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 when Service Now is operating in Direct or Partner Proxy mode or by Service Now partner when Service Now is operating in the End Customer mode. 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.

You can view organizations configured in Service Now on the Organizations page (**Administration > Organizations**) as shown in [Figure 7 on page 99](#).

Figure 7: Organizations Page

Name	Site ID	Submit Cases As	Platform Version	ServiceNow Version	User Name	Connection Status
Test123	—	—	15.1R1.11	16.1R1.375055	test@goopie.com	None Attempted
Test_Org	0100138067	Real Cases	15.1R3.2	16.1R1.375055	super@test.com	Successfully connecte
new_testing_org	0101004067	Real Cases	15.1R3.2	16.1R1.375055	super@test.com	Success
Tests_No_Siteid	None	Real Cases	15.1R3.2	16.1R1.375055	super@test.com	Failed
Tests_21	None	Real Cases	15.1R3.2	16.1R1.375055	super@test.com	Failed

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 [“Service Now Device Groups Overview” on page 111](#).

For more information about creating device groups, see [“Creating a Device Group” on page 112](#).

While you configure organizations to run Service Now in a preproduction environment, you can avoid the processing of production incident cases by operating 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.

[Table 11 on page 100](#) describes the fields displayed in the tabular view of the Organizations page and in the **Organizations Details** dialog box.

Table 11: Organization Column Descriptions

Column Name	Description
Name	Name of the organization.
Site ID	ID of the Customer Site in the Customer Relationship Manager (CRM) of JSS.
Submit Cases As	<p>Specifies whether 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>
Platform Version	<p>Version of Junos Space Network Management Platform used.</p> <p>In a Service Now partner, for an end-customer organization, this field displays the version of Junos Space platform used by the end customer.</p>
Service Now Version	<p>Version of Service Now used.</p> <p>In a Service Now partner, for an end-customer organization, this field displays the version of Service Now used by the end customer.</p>
User Name	<p>Username to identify the user for communication with the JSS while creating cases or checking updates.</p> <p>You do not need to enter a username or password if Service Now is operating in the offline mode.</p>
Connection Status	<p>Status of the connection between Service Now and JSS or Service Now partner.</p> <p>Possible values: Successful or Failed</p>
JMB Filter Level (Only visible in the Detail Summary dialog box, which opens when you double-click the organization)	<p>Filter defining the extent of device information in a JMB to be shared with JSS.</p> <p>Possible values:</p> <ul style="list-style-type: none"> Do not send Device Snapshots—Does not send device snapshots to JSS Send all information except configuration—Sends all device information except the configuration information Send all information with IP Addresses overwritten—Sends all device information with IP addresses overwritten by asterisks Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information <p>NOTE: The Only send list of features used option is applicable for device snapshots or information JMBs (iJMBs) only.</p>



NOTE: Starting in Service Now Release 16.1R1, you can use the Platform Version and Service Now Version fields on the Organizations page to view versions of Network Management Platform and Service Now being used.

Associated Actions

You can perform the following actions related to organizations:

- Add an organization to Service Now; see [“Adding an Organization to Service Now” on page 102](#) 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 104](#) for details.
- View organizations (including end-customer organizations in Partner Proxy mode) configured in Service Now.
- Modify the parameters of an organization; see [“Modifying Organization Parameters” on page 107](#) for details.
- Configure an organization to submit cases as test case; see [“Running an Organization in Test Mode” on page 110](#) for details.
- Test connectivity to JSS or Service Now partner; see [“Testing the Connection to JSS” on page 108](#) for details.
- Delete an organization from Service Now; see [“Deleting an Organization” on page 107](#) for details.
- Associate an organization with an address group; see [“Associating Devices with an Address Group From the Organizations Page” on page 289](#) 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 110](#) 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 109](#) for details.



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

- See Also**
- *Service Now Modes*
 - *Junos Space Service Now Global Settings Overview*
 - [Service Now Address Group Overview on page 285](#)

Creating Organizations

As part of the initial setup of Service Now, 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 102](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 104](#)

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).

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.



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

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 8: 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 103](#).

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 whether cases from this organization should be submitted as real cases or test cases. The synopsis of a test case submitted to JSS or Service Now partner is appended with [Test Mode].	The values are: <ul style="list-style-type: none"> Real cases Test cases 	Real Cases
User Name	Name used to identify the user in JSS while creating cases, and checking for updates to existing cases. You do not need to enter a username or password if Service Now is in the Offline mode.	128 characters; should be in the e-mail address format. Characters can include alphabets, numbers, and the following special characters: ., -, _ and +.	
User Password	Password for the username required for communicating with JSS or Service Now partner. You do not need to enter a username or password if Service Now is in the Offline mode.	32 characters	
Get Sites (button)	Identifier of a site in the Customer Relationship Manager(CRM) of JSS. Click Get Sites and select a Site ID from the Site ID list that is generated when you enter the username and password. NOTE: This option is not available when you add an organization in Service Now operating in the End Customer mode.	80 characters	

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

Name	Description	Range/Length	Default
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 Device Snapshots—Does not send device snapshots to JSS Send all information except configuration—Sends all device information except the configuration information Send all information with IP Addresses overwritten—Sends all device information with IP addresses overwritten by asterisks Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information <p>NOTE: The Only send list of features used option is applicable for device snapshots or information JMBs (iJMBs) only.</p>	—	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**.

Service Now saves the organization and returns to the Organization page.

- See Also**
- [Junos Space Service Now Global Settings Overview](#)
 - [Junos Space Service Now Modes on page 65](#)

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

Junos Space Service Now that is operating in the 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 (referred to as Service Now end customer) should have an organization configured on it. . The Service Now partner provides the username and password for configuring the organization in the 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 9 on page 105](#).

Figure 9: Add Member Dialog Box

Add Member

Name:

User Name:

User Password:

Confirm User Password:

JMB Filter Level:

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 Systems (JSS):

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



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

7. (Optional) Under **Select Configuration**, configure options as follows:

- 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 a Service Now end customer for validation.

If a Service Now partner does not select this check box, the **Configure BIOS Validation** option on the Actions list of Service Now devices is disabled on the Service Now end customer.



NOTE: Starting Service Now Release 15.1R1, the Accept BIOS Validations check box is provided on the Add Member Dialog Box of a Service Now partner to accept or reject BIOS data from Service Now end customers for validation.

- 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.

- See Also**
- [Junos Space Service Now Global Settings Overview](#)
 - [Adding an SNMP Configuration to Service Now on page 194](#)

- See Also**
- [Junos Space Service Now Modes on page 65](#)
 - [Troubleshooting Issues with Adding an Organization to Junos Space Service Now](#)

Modifying Organization Parameters

Junos Space Service Now provides the Modify Organization option to modify the parameters of an organization from the Organizations page on Service Now.

You can modify the following parameters of an organization:

- Name of the organization
- Option to submit cases as test cases or real cases
- Username of the organization
- password of the organization
- Site ID of the organization
- JMB filter level



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 103.

5. Click **Submit**.

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

See Also • [Service Now Organizations Overview on page 99](#)

Deleting an Organization

Junos Space Service Now provides the Delete option on the Actions list of the Organizations page to delete organizations. You cannot delete an organization when the organization is assigned to the default device group.



NOTE: In a Service Now partner, you cannot delete an organization without first deleting end customers associated with the organization..

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**.

Service Now deletes the selected organization from the Service Now database and no longer appears on the Organizations page.



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

See Also • [Service Now Organizations Overview on page 99](#)

Testing the Connection to JSS

Junos Space Service Now provides the Test Connection option on the Actions list to let you test the connection of every organization with Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode).

To test an organization's connectivity with JSS:

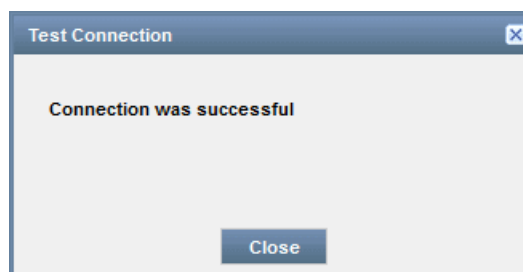
1. From the Service Now navigation tree, select **Administration > Organizations**.

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 or Service Now partner.

Figure 10: 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.

See Also • [Service Now Organizations Overview on page 99](#)

Viewing Messages Assigned to an End Customer

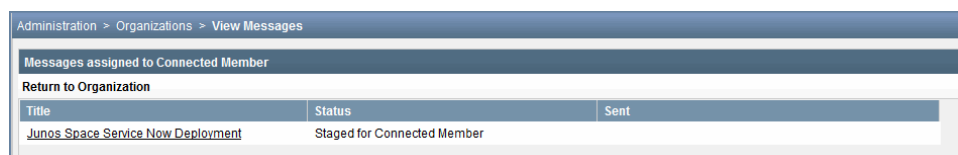
A Service Now partner can view the list of messages that are assigned to an end customer (also known as a connected member). This action is available only when Service Now operates in the Partner Proxy mode and when you select an end customer in the Organizations page.

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 organization for which you want to view the assigned messages.
3. Right-click your selection and select **View Messages** from either the **Actions** list or the right-click menu.

As shown in [Figure 11 on page 109](#), the Messages assigned to Connected Member page displays the list of messages assigned to the selected end customer.

Figure 11: Messages Assigned to Connected Member Page



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 to whom the messages were flagged.

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

- See Also**
- [Assigning a Message to an End Customer on page 355](#)
 - [Service Now Messages Overview on page 353](#)

Running an Organization in Test Mode

While configuring an organization, you can enable test mode to submit cases as test cases so as to avoid processing of test cases by Juniper Support Systems (JSS) or Service Now partner. 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 operate in test mode, and select **Modify Organization** from either the **Actions** list or the right-click menu.

The Modify Organization dialog box displays the parameters of the selected organization.

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

Service Now submits incidents with *[Test]* appended to the incident synopsis for creating cases.

- See Also**
- [Service Now Organizations Overview on page 99](#)

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 an SFTP server for end customers to upload core files, end customers can upload core files to the server used by the Service Now partner. The Service Now partner provides the ID of the case created for an incident to the end customer. The case ID provided by the Service Now partner can be an ID created by the Service Now partner or created by JSS. In either case, the core files are uploaded automatically to the SFTP server once a case is created. For more details, see [“Configuring SFTP Server for Uploading Core Files Generated for Events” on page 198](#).

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 for which you want to configure the server for uploading core files.

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.

- See Also**
- [Service Now Organizations Overview on page 99](#)
 - [Viewing Messages Assigned to an End Customer on page 109](#)

Device Groups

- [Service Now Device Groups Overview on page 111](#)
- [Creating a Device Group on page 112](#)
- [Modifying a Device Group on page 114](#)
- [Deleting a Device Group on page 115](#)


Service Now Device Groups Overview

You can group and manage multiple devices as 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.

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

You can view the device groups configured on Service Now on the Device Groups page (**Administration > Device Groups**) as shown in [Figure 12 on page 111](#).

Figure 12: Core File Upload Configuration Page



Name	Organization	Domain
Device Group for Test_Org	Test_Org	Global
Test	Test_Org	Global

Clicking a device group displays the Device Group Detail page where you can view the details of a device group. [Table 13 on page 112](#) lists the parameters on a device group.

Table 13: Device Group Parameters

Parameter	Description
Name	Name of the device group
Organization	Organization to which the device is assigned
Devices	List of devices assigned to the device group
Auto Submit Policies	List of auto submit policies assigned to the device group
Domain	Domain to which the device group is assigned

Associated Actions

You can perform the following actions related to device groups:

- Create a device group and assign devices to it; see [“Creating a Device Group” on page 112](#) for details.
- Modify device groups; see [“Modifying a Device Group” on page 114](#) for details.
- Delete device groups; see [“Deleting a Device Group” on page 115](#) for details.
- Associate address groups; see [“Associating Devices with an Address Group from the Device Groups Page” on page 290](#) for details.
- Set default device group

- See Also**
- [Service Now Devices Overview on page 117](#)
 - [Service Now Organizations Overview on page 99](#)
 - [Service Now Address Group Overview on page 285](#)

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 or End Customer 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 the default device groups that Service Now creates for organizations.

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.
- Service Now creates a default device group the organization created by an end customer.
- Devices added by end customers are automatically added to the default device group.
- Administrators can edit but not delete the default device group for end customers.

To create a device group:

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

The Create Device Group page appears.

Figure 13: Create Device Group Page

Name	Status	Dampening	Events	Incidents
Test123	Enabled	Disabled	529	0
Test123456	Enabled	Disabled	529	0
ASPTtestREST	Disabled	Enabled	485	0

Note:
Devices added to this Device Group will be automatically associated with the selected Auto Submit Policies.

2. Enter a name for the device group in 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 to associate with this device group.
If you want to associate the device group with a new organization, click **New Organization** and configure the new organization. See [“Adding an Organization to Service Now” on page 102](#) for details.
4. (Optional) In the Select Auto Submit Policies section, select one or more auto submit policies that you want to associate with the device group.
5. Click **Next** to add devices to the device group or click **Finish** to create the device group.
When you click Next, the Add Devices page appears.
6. Select the devices that you want to add to this device group from the **Select Device to add them to the Device Group** section.
7. Click **Finish**.

Service Now adds the selected devices to the device group.

To verify if the devices are added to the device group, double-click the device group on the Device Groups page. The Device Group Detail page lists the devices and auto submit policies that are assigned to the device group.

- See Also**
- [Service Now Devices Overview on page 117](#)
 - [Service Now Auto Submit Policy Overview on page 241](#)

Modifying a Device Group

Service Now provides the Modify Device Group option in the Actions list to modify configured device groups. You can modify the following parameters of a device group:

- Name of the device group
- Organization associated with the device group
- Default status of the device group
- Auto submit policies associated with the device group
- Devices included in the 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 configuration of the selected device group.

Figure 14: Associate Case ID Dialog Box

Administration > Device Groups > Modify Device Group

Edit Device Group

Name:

Organization: [New Organization](#)

Set as Default: ☐

Select Auto Submit Policies

Name	Status	Dampening	Events	Incidents
InitPolicy	0		0	0

Page: 1 of 1 | Displaying 1 - 1 of 1

Device Groups

- Edit Device Group
- Add Devices
- Remove Devices

Back Next Finish Cancel

3. (Optional) In the **Name** text field, modify the name of the device group.
4. (Optional) In the **Organization** drop-down list, modify the organization associated with the device group.

If required, click the **New Organization** button to create a new organization and associate it with the device group. For information about creating a new organization, see [“Adding an Organization to Service Now” on page 102](#).

5. (Optional) Select the **Set as Default** check box to set the device group as the default device group in Service Now.

For Service Now running in Partner Proxy mode, you can set any device group as the default while modifying the device group. 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.**

6. (Optional) Add or remove one or more auto submit policies assigned to the device group by selecting or clearing the check boxes next to the auto submit policies.



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

7. Click **Next** to add devices to the device group or click **Finish** to submit the changes.

If you click Next, Service Now displays the Add Devices page.

8. (Optional) Select one or more devices to add to the device group.
9. Click **Next** to remove devices from the device group or click **Finish** to submit the changes.

If you click Next, the Remove Devices page appears.

10. (Optional) Select one or more devices to be removed from the device group.
11. Click **Finish**.

Service Now modifies the device group and displays the Device Group page.

12. You can verify the changes by double-clicking the modified device group.

The Device Group Detail page appears displaying the devices and auto submit policies assigned to the device group..

- See Also**
- [Service Now Device Groups Overview on page 111](#)
 - [Service Now Devices Overview on page 117](#)

Deleting a Device Group

Junos Space Service Now provides the Delete option in the Actions list on the Device Groups page to delete device groups. You cannot delete a default device group.

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**.

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

- See Also**
- [Service Now Device Groups Overview on page 111](#)
 - [Creating a Device Group on page 112](#)

Service Now Devices

- [Service Now Devices Overview on page 117](#)
- [Adding Devices to Junos Space Service Now on page 123](#)
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
- [Uninstalling an Event Profile from a Device on page 128](#)
- [Exporting Device Data in CSV and Excel Formats on page 130](#)
- [Exporting Inventory Information in CSV Format on page 131](#)
- [Viewing Exposure for a Device on page 132](#)
- [Generating an On-Demand Incident on page 133](#)
- [Collecting RSI and System Log Files on page 138](#)
- [Generating an RMA Incident for a Device on page 142](#)
- [Moving a Device to Maintenance Mode on page 145](#)
- [Deleting a Device from Junos Space Service Now on page 147](#)
- [Associating Devices with a Device Group on page 148](#)
- [Assigning an Auto Submit Policy to a Device on page 148](#)
- [Configuring AI-Scripts Parameters by Using Junos Space Service Now on page 150](#)
- [Viewing Incidents Created for a Device on page 152](#)
- [Verifying the Connection Between a Device and the SFTP Server on page 153](#)
- [Service Now End Customer–Partner Communication Overview on page 153](#)
- [Installing the SSL Certificate on a Service Now End Customer on page 158](#)

Service Now Devices Overview

For Junos Space 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 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 information JMBs (iJMBs) and event JMBs (eJMBs) that help you monitor and resolve issues on the device. You can view devices added to Service Now on the Service Now Devices page (**Administration > Service Now Devices**).

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 a device are displayed under the following five tabs—Details, Address Details, Contract Details, Device Analysis, and Advanced Params Settings..

- 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 the 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](#).

Starting in Service Now Release 16.1R1, a Service Now partner does not send the service contract information for end customer devices to end customers. However, the contract information for end-customer devices can be viewed on the Service Now partner.

- 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
- Advanced Param Settings—Displays AI-Scripts-related configuration for the device

[Table 14 on page 117](#) describes the attributes of Service Now devices displayed under the four tabs.

Table 14: Service Now Devices Field Descriptions

Field Name	Description
Details tab	

Table 14: Service Now Devices Field Descriptions (continued)


Field Name	Description
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.
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
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	Auto submit 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 (JSS); when a device is associated with more than one auto submit policy, 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.

Table 14: Service Now Devices Field Descriptions (continued)

Field Name	Description
Connection Status	Status of connection between the device and Service Now.
Maintenance Mode	<p>Specifies whether the device is currently in maintenance mode or not.</p> <p>Possible values are:</p> <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	<p>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.</p> <p>To receive on-demand updates about your Service Now contract, click the Refresh button on the Device Details page.</p>
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.
Serial Number	Serial number of the device.
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.

Table 14: Service Now Devices Field Descriptions (continued)

Field Name	Description
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 Systems (JSS) or Service Now partner (in case of end customer mode). 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 status 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 status 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 or Service Now partner Validation Success—The validation of BIOS data of the device by JSS or Service Now partner was successful. Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.
Advanced Params Settings	
JMB cleanup age	Number of days after which JMBs are deleted from the device.
Device snapshot collection day of the week	Day of the week when device snapshot should be collected from the device.
Device snapshot collection time of the day	Time of the day when device snapshots should be collected from the device.
Collect logs from all nodes	Indicates if system log files can be collected from all the Service Now devices.
Maximum events to be simultaneously processed on-box	Number of events that AI-Scripts can process when multiple events occur on the device at the same time.
Threshold % of disk usage for warning messages	Percentage of disk used beyond which AI-Scripts should log a warning message indicating that the disk usage has reached the specified threshold.
Threshold % of disk usage for data dampening	Percentage of disk used after which AI-Scripts should not generate JMBs when one or more events occur on the device.

The  icon, when displayed on the left-side of a row on the Service Now Devices page, indicates one of the following scenarios:

- There is a mismatch between the versions of AI-Scripts installed on the 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.

- The device does not have a service contract.



.....

NOTE: Starting in Service Now Release 16.1R1, you see a tool tip on the Service Now Devices page when the device does not have a service contract. In addition to the service contract for the main chassis, Service Now also displays service contracts available for all parts of a device on the Device Details page.

.....

Associated Actions

You can perform the following actions related to Service Now devices:

- View details of a device.
- Add devices from the Junos Space Platform to Service Now; see [“Adding Devices to Junos Space Service Now” on page 123](#) for details.
- Install event profiles on the devices; see [“Installing an Event Profile on a Device by Using Service Now” on page 124](#) for details.
- Uninstall event profiles from the devices; see [“Uninstalling an Event Profile from a Device” on page 128](#) for details.
- Configure BIOS validation; see [“Configuring BIOS Validation for Verifying BIOS Integrity of a Device” on page 162](#) for details.
- Configure product health data collection (PHDC); see [“Configuring Product Health Data Collection on a Device” on page 262](#) for details.
- Export device data in CSV and Excel formats; see [“Exporting Device Data in CSV and Excel Formats” on page 130](#) for details.
- Delete devices from Service Now; see [“Deleting a Device from Junos Space Service Now” on page 147](#) for details.
- Associate devices with a device group; see [“Associating Devices with a Device Group” on page 148](#) for details.
- Associate auto submit policies with devices; see [“Assigning an Auto Submit Policy to a Device” on page 148](#) for details.
- Export inventory information in CSV format; see [“Exporting Inventory Information in CSV Format” on page 131](#) for details.
- View the devices that are susceptible to known issues; see [“Viewing Exposure for a Device” on page 132](#) for details.
- Generate on-demand incidents; see [“Generating an On-Demand Incident” on page 133](#) for details.
- Generate on-demand device snapshot; see [“Generating an On-Demand Device Snapshot” on page 359](#)
- Request RMA incidents; see [“Generating an RMA Incident for a Device” on page 142](#) for details.

- Associate devices with an address group; see [“Associating Devices with an Address Group from the Service Now Devices Page”](#) on page 292 for details.
- Verify the connection between the devices and the SFTP server; see [“Verifying the Connection Between a Device and the SFTP Server”](#) on page 153 for details.
- View incidents created for a device; see [“Viewing Incidents Created for a Device”](#) on page 152 for details.
- Configure RSI and log file collections; see [“Collecting RSI and System Log Files”](#) on page 138 for details.
- Assign a device to another domain; see [“Assigning a Service Now Object to a Domain”](#) on page 58 for details.
- Move a device to maintenance mode; see [“Moving a Device to Maintenance Mode”](#) on page 145 for details.

- See Also**
- [Service Now Device Groups Overview](#) on page 111
 - [Service Now Event Profiles Overview](#) on page 165
 - [Service Now Auto Submit Policy Overview](#) on page 241
 - [Service Now BIOS Validation Overview](#) on page 160
 - [Product Health Data Collection Configuration Overview](#) on page 259
 - [Service Now Incidents Overview](#) on page 302

Adding Devices to Junos Space Service Now

Junos Space Service Now adds devices discovered by Junos Space Network Management Platform automatically if the devices are discovered after Service Now is installed on Junos Space Platform. However, if you discover devices after Service Now is installed, you have manually add the discovered devices to Service Now.

Service Now provides the Add Devices option in the Service Now Devices task of the Service Now navigation tree to add devices.

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 15: Select Devices to Add to Service Now and Click Submit Page

Select Devices to Add to Service Now and Click Submit				
Host Name	IP Address	Serial Number	Product	Version
<input checked="" type="checkbox"/> p26-p2	192.0.2.1	xxxxxxxxxx	ACX2000	12.3-20130929_acx_x51_s1.0

Page 1 of 1 | Displaying 1 - 1 of 1

2. Select the devices that you want to add.

3. Click **Submit**.

The Service Now Devices page appears and lists the devices added to Service Now..

- See Also**
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
 - [Assigning an Auto Submit Policy to a Device on page 148](#)
 - [Juniper Networks Devices Supported by Service Now and Service Insight on page 25](#)

Installing an Event Profile on a Device by Using Service Now

An event profile defines a set of event policies selected from an AI-Scripts bundle to generate Juniper Message Bundles (JMBs) for informing users about an event when the event occurs on a device.. When you install an event profile on managed devices, the event policies detect the events that occur on devices and automatically provide the information needed to troubleshoot the events.


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.
- For information about behavior of AI-Scripts when installed on specific product families, see <https://kb.juniper.net/InfoCenter/index?page=content&id=KB29188>.

The  icon appears on the left side of a device row on the Service Now Devices page if the versions of the AI-Scripts installed on the device and Service Now are different. For a device with 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:

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 navigation tree, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

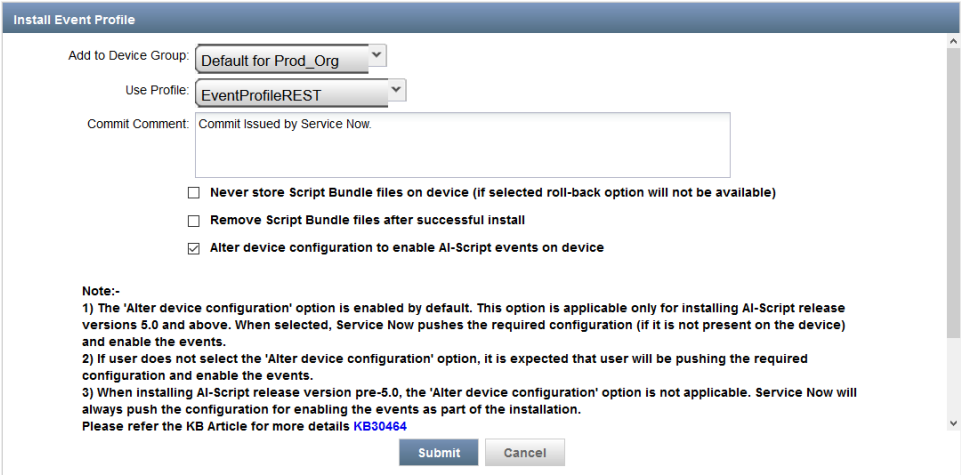
2. Select the device on which you want to install the event profile.

The Install Event Profile action is active even if the devices are not associated with an organization or Device Group.

3. From the Actions list or right-click menu, select **Device Operations > Install Event Profile**.

The Install Event Profile page appears as shown in [Figure 16 on page 125](#).

Figure 16: Install Event Profile Page



Install Event Profile

Add to Device Group: Default for Prod_Org

Use Profile: EventProfileREST

Commit Comment: Commit Issued by Service Now

☐ 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](#)

Submit Cancel

4. Select a device group from the **Add to Device Group** drop-down list to add the device to the device group.
5. Select an event profile from the **Use Profile** drop-down list to assign to the device.
6. (Optional) Enter your comments for installing the event profile in the **Commit Comment** text box.

The maximum number of characters allowed is 225. Service Now adds a default comment as **Commit Issued by Service Now for enabling AI-Scripts**.



NOTE: This option is not available if the **Alter device configuration to enable AI-Script events on device** check box is not selected.

When a Service Now device is deleted from Service Now, the commit comment present in the Advanced Settings page is used while committing AI-Scripts configuration on a device.

You can view the commit comment on a device by executing the **show system commit** command.

7. (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.

8. (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.

9. (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.

10. (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.

11. Click **Submit**.

12. (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.

13. Click **Finish**.

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

14. 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:

- Click the **Apply this Event Profile to Devices manually** link.
- Click the devices on which you want to apply the event profile.
- 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.

- 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.

- See Also**
- [Service Now Event Profiles Overview on page 165](#)
 - [AI-Scripts Overview on page 35](#)
 - [Manually Installing AI-Scripts on Devices on page 46](#)
 - [Adding a Script Bundle to Junos Space Service Now on page 188](#)
 - [Viewing Exposure for a Device on page 132](#)

Uninstalling an Event Profile from a Device

Junos Space Service Now provides the Uninstall Event Profiles from managed devices option in the Actions list of the Service Now Devices page to uninstall event profiles. . 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.



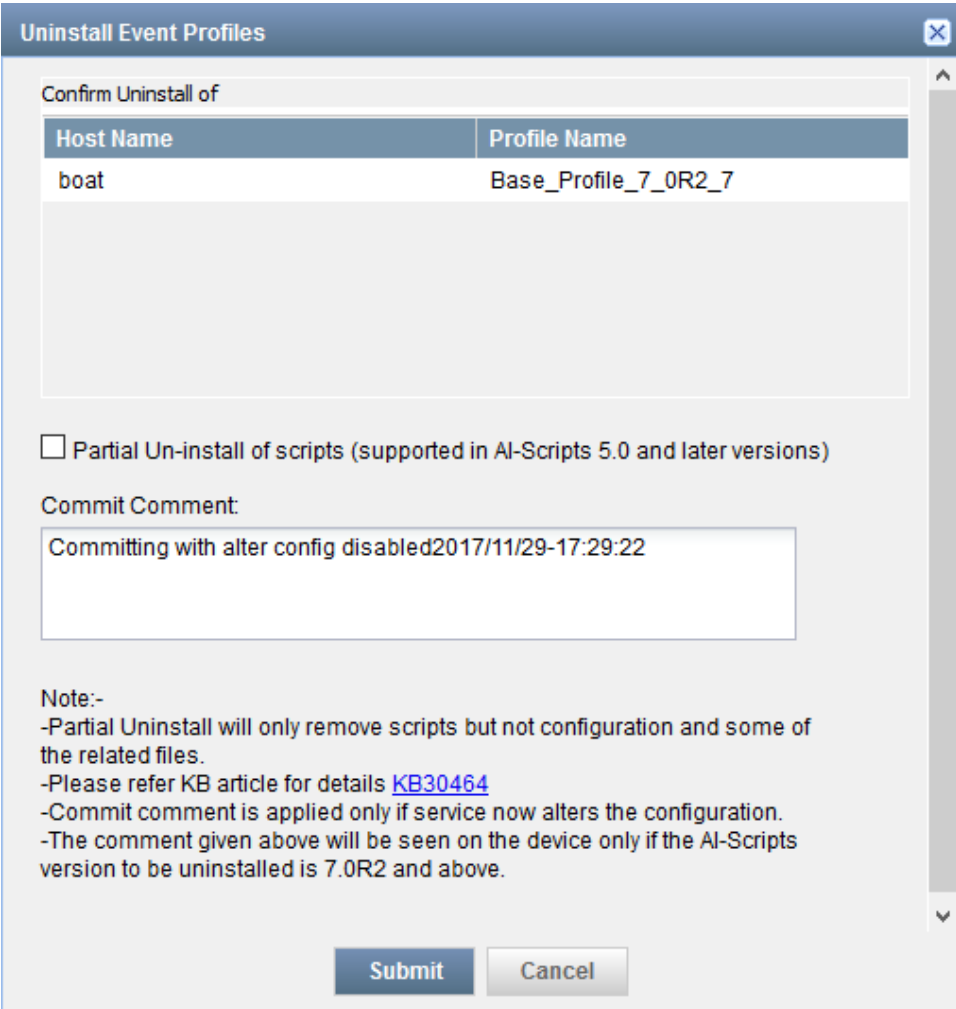
NOTE: A Service Now partner cannot uninstall event profiles from a Service Now end-customer's devices.

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 list or right-click menu, select **Device Operations > Uninstall Event Profile**.

The Uninstall Event Profile dialog box appears as shown in [Figure 17 on page 129](#).

Figure 17: Uninstall Event Profiles Dialog Box



The dialog box is titled "Uninstall Event Profiles". It 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 text box for a "Commit Comment". At the bottom, there is a "Note" section with several bullet points and two buttons: "Submit" and "Cancel".

Host Name	Profile Name
boat	Base_Profile_7_0R2_7

☐ Partial Un-install of scripts (supported in AI-Scripts 5.0 and later versions)

Commit Comment:

Committing with alter config disabled2017/11/29-17:29:22

Note:-

- Partial Uninstall will only remove scripts but not configuration and some of the related files.
- Please refer KB article for details [KB30464](#)
- Commit comment is applied only if service now alters the configuration.
- The comment given above will be seen on the device only if the AI-Scripts version to be uninstalled is 7.0R2 and above.

Submit **Cancel**

4. (Optional) Enter your comments for uninstalling the event profile in the **Commit Comment** text box.

The maximum number of characters allowed for a comment is 225. Service Now enters a default comment as **Commit Issued by Service Now for disabling AI-Scripts**.



NOTE: This option is available from AI scripts 7.0R2 and later installed on Service now 17.1R1 and later.

When you delete a device from Service Now, AI-Scripts configuration is first deleted from the device. While deleting the AI-Scripts configuration, the commit comment provided on the Advanced Settings page is used as the comment for committing the AI-Scripts configuration on the device.

You can view the commit comment on a device by executing the **show system commit** command.

5. Select the **Partial Un-install of scripts(Supported in AI-Script 5.0 and above versions)** check box 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 of Junos OS on the device).

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

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

See Also • [AI-Scripts Overview on page 35](#)

Exporting Device Data in CSV and Excel Formats

Junos Space Service Now provides the Export Devices option on the Actions list of the Service Now devices page to export Service Now device data in CSV or Excel file formats.

Service Now exports the following information about a device:

- Host name of the device
- IP address of the device
- Device group to which the device is assigned
- Organization associated with the device
- Organization associated with the end customer device when the device is an end customer device (
- Product family to which the device belongs
- Routing software installed on the device
- Serial number of the device
- Version of the routing software
- AI-Scripts version installed on the device
- Event profile installed on the device
- Date and time the event profile was installed on the device
- Location of the device
- Address where the RMA parts for the device should be shipped
- Domain to which the device is assigned

- Auto submit policy assigned to the device
- Whether or not the device is operating in the maintenance mode
- RSI file configuration of the device
- Log file configuration of the device

To export the device data in CSV or Excel format:

1. From the Service Now navigation tree, select **Administration > Service Now Devices**.
The Service Now Devices page appears.
2. Select one or more devices whose data you want to export, and select **Export Devices** from either the **Actions** list or the right-click menu.



TIP: To export data of all devices in Service Now, select the check box on the header of the table on the Service Now devices page.

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.

The browser displays the dialog box to open or save the file

4. Open or save the file at a desired location.

- See Also**
- [Service Now Devices Overview on page 117](#)
 - [Deleting a Device from Junos Space Service Now on page 147](#)
 - [Assigning an Auto Submit Policy to a Device on page 148](#)

Exporting Inventory Information in CSV Format

A Service Now partner can export a customer's device inventory information to CSV or Excel file format.

Service Now exports the following inventory information to the CSV or Excel file—device name, item, model number, part number, serial number, contract number, service SKU, contract start, contract end and description.



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

To export the inventory information:

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

The Service Now Devices page appears.

2.
 - To export inventory of selected devices, select the device and click **Export Inventory Information** either from the **Actions** list or the right-click menu.
 - To export inventory of all devices in Service Now, select **Export Inventory Information** either from the **Actions** list or the right-click menu.

The Export Inventory Information dialog box is displayed.

3. Export the inventory information:

- Click the **Export Inventory Information in CSV format** link to export the inventory information for selected devices to a CSV file.
- Click the **Export All Inventory Information in CSV format** link to export the inventory information for all devices in Service Now to a CSV file.
- Click the **Export Inventory Information in Excel format** link to export the inventory information for selected devices to an Excel file.
- Click the **Export All Inventory Information in Excel format** link to export the inventory information for all devices to an Excel file.

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

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

See Also • [Service Now Devices Overview on page 117](#)

Viewing Exposure for a Device

The Service Now Devices page displays an alert (!) icon before the Organization column of devices for which advisories (also known as Install Advisor or exposure) are issued for installing AI-Scripts.

The Install Advisor is an advisory created by Juniper Support Systems (JSS) to advise you of any issues with AI-Scripts on the Junos OS versions running on devices managed by Service Now. The advisory includes a number and link to the problem report (PR) that describes the issue, a message, product model, and information about the Junos OS and AI-Scripts version that have the issue.

Service Now retrieves advisories from JSS once every 24 hours and scans all the devices managed by it to check if the devices match the parameters (product model, Junos OS version, and AI-Scripts version) mentioned in the advisory. If there is a device matching the parameters specified in the advisory, Service Now displays an alert icon for that device on the Service Now Devices page. Clicking the alert icon displays a warning message indicating the device has known issues.

The alert icon is also displayed for a device when a version of AI-Scripts that has an advisory issued is selected for installing on the device.



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

To view advisory or exposure for a device:

1. On the Service Now navigation tree, 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 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 the link in the PR column to view the issue and take suitable actions.

Clicking the link opens the Problem Report Search tool and displays the details of the PR.

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

See Also • [Service Now Devices Overview on page 117](#)

Generating an On-Demand Incident

By using Junos Space Service Now, you can create Juniper Message Bundles (JMBs) for devices without having to wait for an event to occur on the device. 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 Systems (JSS) for creating a case. To avoid submitting incidents automatically, clear the **Automatically Submit Cases** check box present on the On-demand Incident dialog box displayed while creating the on-demand JMB.



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.
 - You cannot create an on-demand incident for a device if the device is not associated with a device group.
-

Starting Junos Space Service Now 17.1R1 release, you can associate a new on-demand incident with technical support cases that are not closed. When an incident is associated with a case, the ID of the case is displayed in the Case Details tab of the Incident Details page and the Incidents page displays the Status of the incident as **Case Associated** along with the case ID with which the incident is associated. The attachments and log files of the incident are uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode) and associated with the related case.



NOTE:

- To associate an incident to a case, the case should not be in the Closed state.
 - Once an incident is associated with a case, the association cannot be undone.
 - An incident in one domain can be associated with a case assigned to another domain. A case can be associated with multiple domains.
-

To generate an on-demand incident:

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

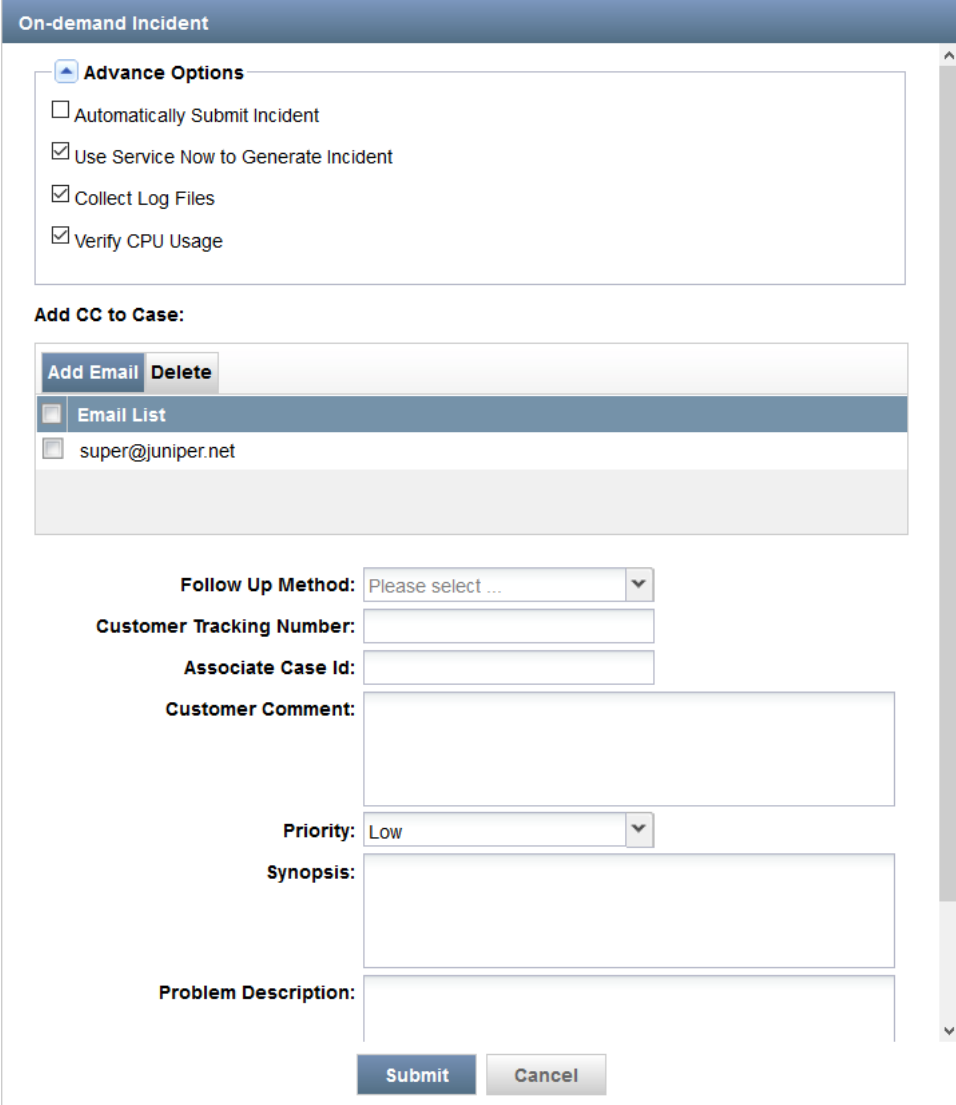
2. On the Service Now Devices page, select the device for which you want to generate an on-demand incident.

3. From the Actions list or the right-click menu, select **Device Operations > 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 18 on page 135](#).

Figure 18: On-demand Incident Dialog Box



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

- Advance Options:** A section with four checkboxes:
 - ☐ Automatically Submit Incident
 - ☒ 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 table:

Email List
super@juniper.net
- Follow Up Method:** A dropdown menu with the text "Please select ...".
- Customer Tracking Number:** A text input field.
- Associate Case Id:** A text input field.
- Customer Comment:** A large text area.
- Priority:** A dropdown menu with the text "Low".
- Synopsis:** A text input field.
- Problem Description:** A large text area.
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

- (Optional) At the top of the On-demand Incident dialog box, clear the **Automatically Submit Incident** check box to avoid submitting incidents to JSS or Service Now partner automatically, or to associate the incident with a technical support case.



NOTE: The **Automatically Submit Incident** check box is selected by default.

- (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 15 on page 136](#), 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 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



NOTE: The Collect Log Files and Verify CPU Usage fields are not visible on the On-demand Incidents page if Service Now is operating in the End Customer mode.

6. Under Email List, click the **Enter Email Id** check box to enter an e-mail ID in the `user@example.com` format.
Service Now sends a copy of the on-demand incident to the configured e-mail IDs.
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. Enter the customer tracking number in the **Customer Tracking Number** field.
Customer tracking number is a user-defined number assigned for tracking incidents and cases.

10. (Optional) To associate the on-demand incident with an existing technical support case, enter the Case ID of the technical support case in the **Associate Case Id** field.



NOTE:

- You can associate an on-demand incident with a technical support case only if the case is in the open state.
- This field is visible only when the Automatically Submit Incident check box is not selected.

11. (Optional) Enter a comment when you associate the selected incidents with the case in the **Customer Comment** text field.

The customer comment along with incident information appears as case notes (incident information listed first followed by the customer comment) in Case Manager. Service Now auto-generates the incident information and sends the incident information and customer comment to Case Manager.

Total number of characters allowed in a customer comment is 38000.



NOTE: This field is visible only when the Automatically Submit Incident check box is not selected.

12. Select the priority of the case from the **Priority** list.

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

13. In the **Synopsis** field, enter a synopsis of the on-demand incident.

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



NOTE: The values for the fields listed in step 6 through step 12 are already defined on the basis of the incident that is generated by the selected profile. You can modify these values if needed.

14. In the **Problem Description** field, enter a description of the on-demand incident.

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

15. (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.

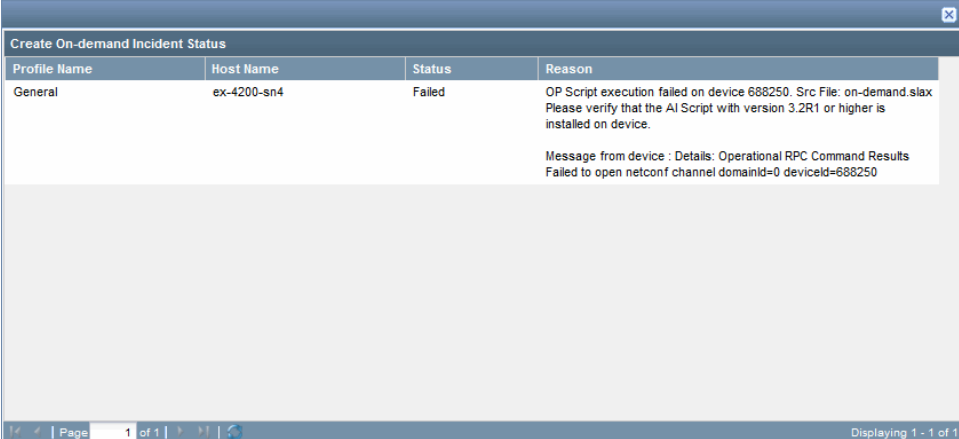
If you do not schedule a time, the on-demand incident is created immediately after you complete configuring the on-demand incident.

16. 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 19 on page 138](#)), 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 19: 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

See Also • [Service Now Incidents Overview on page 302](#)

Collecting RSI and System Log Files

Junos Space 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 within the configured interval after RSI is collected, Service Now uses the already collected RSI in the JMB of those events.



NOTE: Service Now executes the RSI brief command on devices running subscriber management services instead of the regular RSI command to avoid impacting the performance of device CPU.

The RSI brief command does not execute the detail option due to which size of the output is smaller as compared with the output of regular RSI command.


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 are displayed. You must manually delete these files from the device.

- 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.
- We recommend that you configure RSI collection at least once by using Service Now to ensure proper generation of the RSI attachment for a JMB.

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 list or right-click menu, select **Configure File Collection**.

The Configure File Collections dialog box appears as shown in [Figure 20 on page 140](#).

Figure 20: Configure File Collections Dialog Box

Configure File Collections

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

RSI

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

5 mins

Log Files

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

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

Submit **Cancel**

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

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

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

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

- Service Now is configured to collect RSI once 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.
- By 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. If you have scheduled a time, the job for creating the on-demand incident is initiated at the scheduled time.
8. (Optional) In the Job Information dialog box, click the job ID link to view the status of the job.

See Also • [AI-Scripts Overview on page 35](#)

Generating an RMA Incident for a Device

You can use the off-box feature in Service Now to generate Return Materials Authorization (RMA) incidents for a device. With the off-box feature, Service Now generates RMA incidents using the preloaded **directive.rc** file. In a Service Now operating in the Partner Proxy mode, you cannot create an RMA incident for end-customer devices by using the off-box feature..



NOTE: Currently, this feature is not supported on devices that are not associated with a device group.

Starting Junos Space Service Now 17.1R1 release, you can associate a new RMA incident with technical support cases that are not closed. When an incident is associated with a case, the ID of the case is displayed in the Case Details tab of the Incident Details page and the Incidents page displays the Status of the incident as **Case Associated** along with the case ID with which the incident is associated. The attachments and log files of the incident are uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode) and associated with the related case.



NOTE:

- To associate an incident to a case, the case should not be in the Closed state.
- Once an incident is associated with a case, the association cannot be undone.
- An incident in one domain can be associated with a case assigned to another domain. A case can be associated with multiple domains.

To generate 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 generate an RMA incident.
3. From the Actions list or the right-click menu, select **Device Operations > 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 21 on page 143](#).

Figure 21: Request RMA page

4. (Optional) At the top of the Request RMA page, clear the **Automatically Submit Incident** check box if you do not want to submit RMA incidents automatically to Juniper Support Systems (JSS) or Service Now partner, or associate the incident with a technical support case..



NOTE: The **Automatically Submit Incident** check box is selected by default.

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 16 on page 143](#), 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 16: 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.

Service Now sends a copy of the RMA incident to the configured e-mail IDs.

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. Enter the customer tracking number in the **Customer Tracking Number** field.

Customer tracking number is a user-defined number assigned for tracking incidents and cases.

11. (Optional) To associate the RMA incident with an existing technical support case, enter the Case ID in the **Associate Case Id** field.



NOTE:

- You can associate an RMA incident with a technical support case only if the case is in the open state.
- This field is visible only when the Automatically Submit Incident check box is not selected.

12. (Optional) Enter a comment for associating the selected incidents with the case in the **Customer Comment** text field.

The customer comment along with incident information appear as case notes (incident information listed first followed by the customer comment) in Case Manager. Service Now auto-generates the incident information and sends the incident information and customer comment to Case Manager.

Total number of characters allowed in a customer comment is 38000.



NOTE: This field is visible only when the Automatically Submit Incident check box is not selected.

13. From the **Priority** list, select the priority of the case.

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

14. In the **Synopsis** field, enter a synopsis of the RMA incident.

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

15. 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.

16. Select the address group from the **Address Groups** list.

The address group indicates the address to which the replacement part should be shipped.

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.

The **Ship-to Address** field is auto-populated with the address configured in the selected address group.

17. 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. The selected components appear in the **Request RMA Parts** text box.

18. (Optional) If you want to schedule generating the RMA incident at a later time, select the **Schedule at a later time** check box and enter the date and time for the schedule.

19. Click **Submit**.

Service Now initiates a job to create an RMA incident.

If you have scheduled a time for creating the RMA incident, Service Now initiates the process to create the RMA incident at the scheduled time.

See Also • [Service Now Incidents Overview on page 302](#)

Moving a Device to Maintenance Mode

Starting Junos Space Service Now Release 15.1R1, Service Now provides the Maintenance Mode option on the Actions list 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 tasks when a managed device is placed in maintenance mode:

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

When operating in the End Customer mode, Service Now 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.
- 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 list, 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 22 on page 146](#).

Figure 22: 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, select one of the following options:
 - **Selected device(s)** to move devices selected on the Service Now Devices page to the maintenance mode
 - **All managed devices in the current domain** to move all the managed devices in the current domain to maintenance mode.
 6. (Optional) 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.

See Also • [Service Now Devices Overview on page 117](#)

Deleting a Device from Junos Space Service Now

Junos Space Service Now provides the Delete option on the Actions list of the Service Now Devices page to delete a device from Junos Space Service Now database. When you delete a device, the device is deleted only from the Junos Space Service Now database along with its related incidents and JMBs. The device is not deleted from Junos Space Network Management Platform.

When you delete a device that has AI-Scripts installed on it from Service Now, the AI-Scripts package is 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** list or the right-click menu.

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**.

Service Now deletes the selected devices from the Service Now database and does not display it on the Service Now Devices page.

See Also • [Service Now Devices Overview on page 117](#)

Associating Devices with a Device Group

Junos Space Service Now provides the Associate Device Groups option on the Actions list of the Service Now devices page to can associate devices with device groups. 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 end 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 a 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.

See Also • [Device group Overview](#)

Assigning an Auto Submit Policy to a Device

Auto submit policies allow Service Now to submit incidents automatically to Juniper Support Systems (JSS) or Service Now partner for creating cases. 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 243](#).

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 23: Modify Auto Submit Policy Page

3. Under the Select Policy section, select the auto submit policies that you want to assign to the selected devices.



TIP: Click the check box next to Select Policy to select all auto submit policies for assigning to the selected devices.

4. To assign auto submit policies to selected devices, click **Add**.



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

The Service Now Devices page appears. Service Now displays the auto submit policies to which a device is assigned in the auto submit policy column.

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

- See Also**
- [Service Now Auto Submit Policy Overview on page 241](#)
 - [Adding Devices to Junos Space Service Now on page 123](#)
 - [Service Now Devices Overview on page 117](#)
 - [Collecting RSI and System Log Files on page 138](#)

Configuring AI-Scripts Parameters by Using Junos Space Service Now

AI-Scripts parameters such as duration after which a JMB should be deleted from the device, day and time for collecting intelligence JMBs (or device snapshots), and so on are configured by using the `ais-param-set.slax` file that is present in the AI-Scripts bundle. Starting Junos Space Service Now Release 17.2R1, Service Now provides the Advanced Parameters Settings option in the Actions list to configure the AI-Scripts parameters from the Junos Space Service Now GUI.



NOTE: We recommend that you configure AI-Scripts parameters on a device by using Service Now after you consult with [Juniper Networks support team](#).

To configure AI-Scripts parameters from the Service Now GUI:

1. From the Navigation tree, navigate to **Administration > Service Now Devices**.

The Advanced Parameters Settings dialog box appears.

2. Select one or more devices on which you want to configure the AI-Scripts parameters and select **Device Operations > Advanced Parameters Settings** from the Actions list or the right-click menu.

The Advanced Parameter Settings for AI-Script dialog box appears as shown in [Figure 24 on page 151](#).

Figure 24: Advanced Parameters Settings for AI-Scripts

Advanced Parameters Settings for AI-Scripts

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

Note: This is supported from AI-Script version 5.0 and above.

Advanced Settings

Age of JMB before it is deleted if not picked up by Service Now (in days): 3

Device snapshot collection day of the week: Monday

Device snapshot collection time of the day: 1:09 AM

Maximum events to be simultaneously processed on the device: 8

Threshold percentage of disk usage for warning messages: 50

Threshold percentage of disk usage for JMB/Attachment dampening: 75

Collect logs from all nodes: ☐ Yes ☒ No

☐ Apply to all Service Now managed devices

☐ ☒ Schedule Configuration on selected device(s) at specified time: _____

Submit Cancel

3. If the AI-Scripts parameters are not visible, click the down arrow next to Advanced Settings to view AI-Scripts parameters.

The AI-Scripts parameters are displayed.

4. Enter values for the AI-Scripts parameters as follows:

- **Age of before it is deleted if not picked up by Service Now (in days):** Select the number of days after which AI-Scripts should delete JMBs from the device.
- **Device snapshot collection day of the week:** Select the day of the week when AI-Scripts should execute scripts for collecting device snapshot from the device.
- **Device snapshot collection time of the day:** Select a time of the day from when AI-Scripts should execute scripts for collecting device snapshot from the device.

This list provides values at an interval of 15 minutes. You can also enter any value other than the listed values; for example, 1:10 AM, 2:20 AM, 4:05 PM, and so on.

- **Maximum events to be simultaneously processed on the device:** Select the number of events that AI-Scripts can process when multiple events occur on the device at the same time.

You can configure values from 1 to 15.

- **Threshold percentage of disk usage for warning messages:** Enter the disk usage limit, in terms of percentage, beyond which AI-Scripts should log a warning message to indicate that the disk usage has reached the specified threshold.

- **Threshold percentage of disk usage for JMB/Attachment dampening:** Enter the disk usage limit, in terms of percentage, after which AI-Scripts should not generate JMBs when one or more events occur on the device.
 - **Collect logs from all nodes:** Select **Yes** to allow AI-Scripts to collect system log files from all devices or select **No** to prevent AI-Scripts from collecting system log files.
5. (Optional) Select the **Apply to all Service Now managed devices** check box to configure the AI-Scripts parameters on all devices managed by Service Now.
 6. (Optional) Select the **Schedule Configuration on selected device(s) at specified time** check box to schedule a date and time for configuring the AI-Scripts parameters.
 7. Click **Submit**.

If you have provided a schedule to configure the AI-Scripts parameters, Service Now configures the AI-Scripts parameters at the scheduled time. Otherwise, Service Now creates a job for configuring the AI-Scripts parameters on the selected devices immediately after you click Submit.

- See Also**
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
 - [Adding a Script Bundle to Junos Space Service Now on page 188](#)
 - [AI-Scripts Overview on page 35](#)

Viewing Incidents Created for a Device

Junos Space Service Now creates incidents when it receives a JMB from a device. You can view the incidents on the Incidents page of the Service Central workspace.

To view incidents created in 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 a device to view the incidents that Service Now has created.



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 incident details, see [“Service Now Incidents Overview” on page 302](#).

Alternatively, you can view all the incidents created for all devices on the Service Now dashboard.

- See Also**
- Incidents Overview
 - Service Central Overview

Verifying the Connection Between a Device and the SFTP Server

Junos Space Service Now uploads core files generated as a part of a JMB to an SFTP server. When there is an issue in uploading core files, you can verify the connection between the devices and the SFTP server.



NOTE: You cannot verify the connection between a device and the SFTP Server by using Service Now when Service Now is operating in the End Customer mode.

To verify the connection between the device and the SFTP 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 want to verify the connection with the SFTP server, 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.

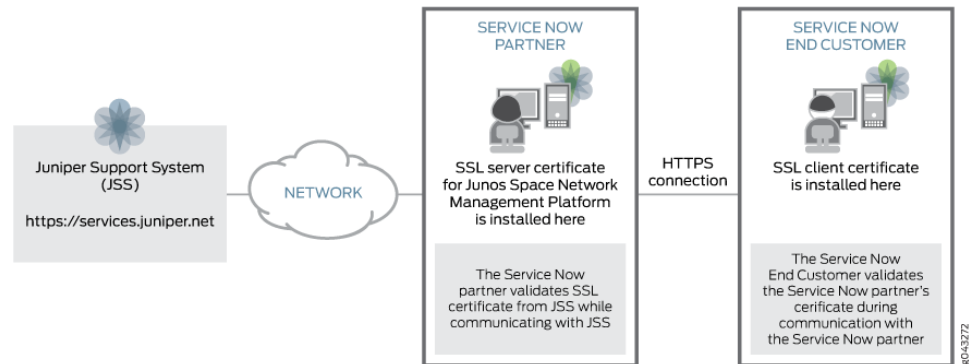
- See Also**
- Configuring Core file Upload
 - [Configuring SFTP Server for Uploading Core Files Generated for Events on page 198](#)
 - [Updating Core File Upload Configuration for an End Customer on page 110](#)

Service Now End Customer–Partner Communication Overview

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

[Figure 25 on page 154](#) depicts the communication between a Service Now partner with a Service Now End Customer and Juniper Support Systems (JSS) by using an SSL certificate.

Figure 25: Service Now Partner Communicating with a Service Now End Customer and JSS Using SSL Certificate



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

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

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

1. [Generating CSR by Service Now Partner on page 154](#)
2. [Obtaining Signature of a Certificate Authority on page 157](#)
3. [Uploading the Certificate to Service Now Partner on page 157](#)
4. [Obtaining the Intermediate Certificate \(key\) for Establishing Credibility of the SSL Certificate on page 157](#)
5. [Obtaining SSL Certificate of the Service Now Partner on page 157](#)

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  
AV7Ln6hg8Jl+UPEbrZPvXVED29qvM4tp1SDwKwuLs+IRWsON9ee2TsmVubCE0Ac7  
aA8jg7kzubCktF3y+8/1M3yf+IWMy4EdWBXWtjMBO22kjU5KGwyznQeCsN2HtOLp  
WvFOFDQHgxougL0qfF7pkDsVby5bKv740T+ju/On6HtLf8IUfZDh/Xui/scsoKeb  
8eJnKN01dYAtU+eyNwkmP1o9j8Ly/Geei00amMFaDp01WuMQLmEH8En3tVIULrD  
WZ2Ly0U9+d6J16f7LXXIEcBcH0e00C3pp7Bq4z1k0/2WPq5FmcM90mZZdeC2ZeYP  
fNzBk21ZVVDAM89ggN1RNsm6FG9F6kkfczjB0SvawhBs7AgTDzty5J279uTGIyo1  
1CVXbijo9+KR3INX3nWatYYR7T7MUG1Yma/MbCg2dWAPR6iwYWy3w6VD51BIGNCP  
po42Y0H4yLvT80uVzkpQ8z9tjuk05ZAR6E8fWEdiYBbPIhfEBxc7WVUBdPE/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  
BxMGU31kbmV5MRAwDgYDVQQKEwdKdW5pcGVyMQswCQYDVQQLEwJBZUzEPMA0GA1UE  
AxMGAUtbWfUMR8wHQYJKoZIhvcNAQkBFhBmcMvKQCp1bm1wZXIubmV0MIGfMA0G  
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCjA2megTM4/9iP9I56iNqmKmROQYfPwHLn  
pW7BWq1Dikzn8BqM6cFeMa1vUpRntiPJRNbUjGZPbfa3cwZEy/vgy3MyTALFj9Zy  
7tkpUId1Qn2KhW47mEcaixkEec5PxOUZm3Af1kKcMtIzaJxyVRS6cr6xLy0Bqew  
1TA+3Xj6PwIDAQABoBkwFwYJKoZIhvcNAQkHMqoTCGZyZWQxMjMOMAOGCSqGSIb3  
DQEBBQUAA4GBAJjxApGFYAFu11x0osdoGzedRkrVmR5693+h0EtI01n0z7ONCVu  
ix0in4dH0SDipNPgfZwQ0jx6wyVGx/b6wWpMxBTrvhxH1EiCgr9pP0U63eMZsyEI  
3RoU+7KERTxxtXbRYUx0EHGPD0HSgiShbjVc2uAPXijSR1utI3sViTJ2  
-----END CERTIFICATE REQUEST-----
```

Obtaining Signature of a Certificate Authority

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



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

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

Uploading the Certificate to Service Now Partner

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

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

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

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

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

Obtaining SSL Certificate of the Service Now Partner

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



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

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

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

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

3. Click **More Information**.

The Page Info dialog box appears.

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

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

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

The Save To dialog box of the web browser appears.

6. Save the certificate on your local system.

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

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

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

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

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

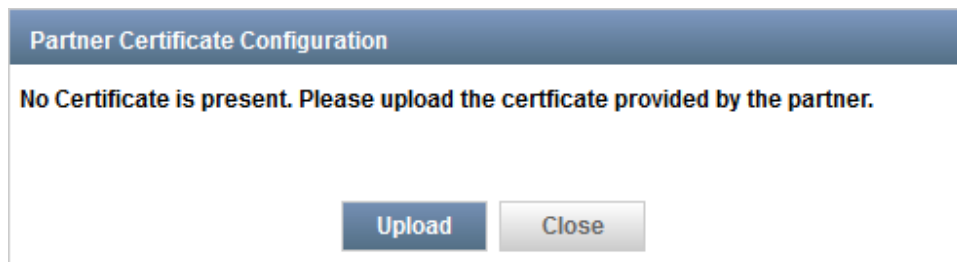
See Also • [Installing the SSL Certificate on a Service Now End Customer on page 158](#)

Installing the SSL Certificate on a Service Now End Customer

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

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

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

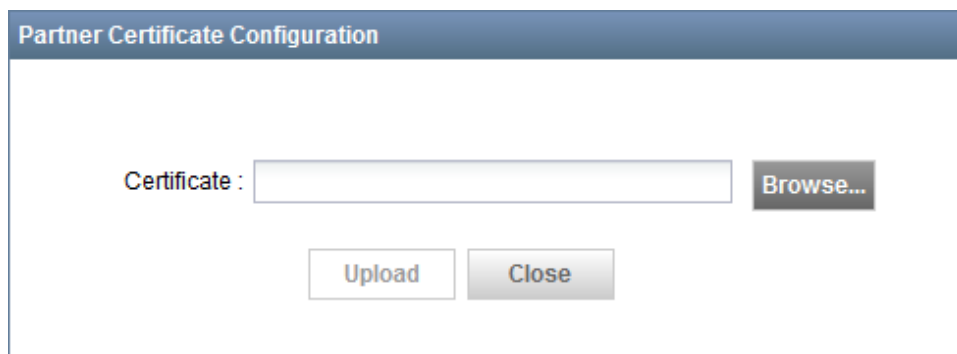


Partner Certificate Configuration

No Certificate is present. Please upload the certificate provided by the partner.

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

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



Partner Certificate Configuration

Certificate :

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 Netwc"
- Issuer Name:** EMAILADDRESS=root@192.0.2.166 CN=192.0.2.166 , OU=Junos Space, O="Juniper Netwc"
- 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 right, there are two buttons: 'Delete Certificate' and 'Close'.

See Also • [Certificate Management Overview](#)

BIOS Validation

- [Service Now BIOS Validation Overview on page 160](#)
- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 162](#)

Service Now BIOS Validation Overview

Junos Space Service Now provides the BIOS validation option to 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, Service Now creates BIOS validation incidents (**Service Central > Device Analysis > BIOS Validations**) and submits the BIOS data to Juniper Support Systems (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 104.

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 26 on page 161](#) and [Figure 27 on page 162](#) show the legal notice displayed on Service Now operating in Partner Proxy and End Customer modes respectively.

Figure 26: BIOS Validation Legal Notice on Service Now Partner

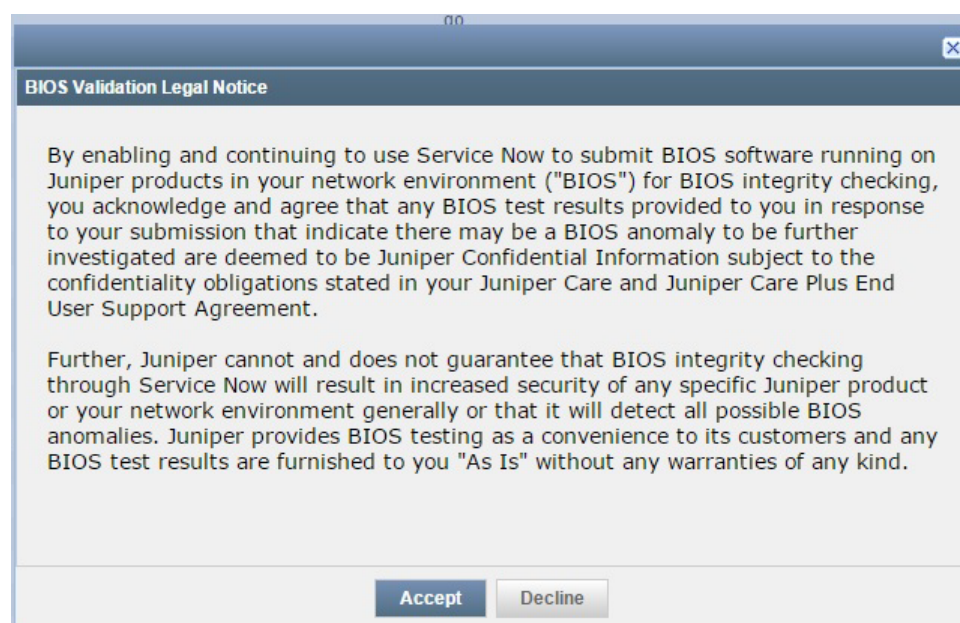
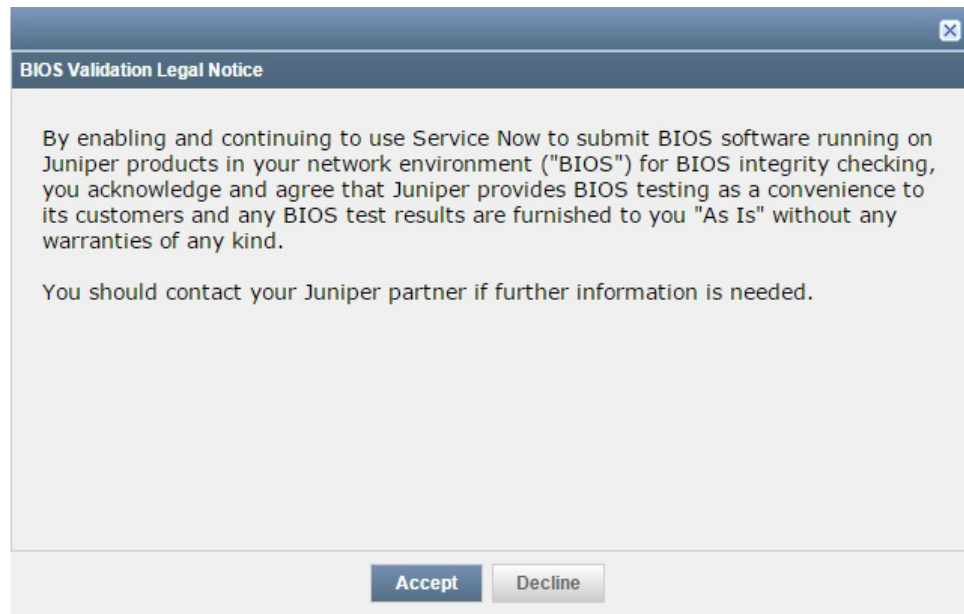


Figure 27: BIOS Validation Legal Notice on Service Now End Customer

Associated Actions

You can perform the following actions related to BIOS validation:

- View BIOS validation incidents; see ["Viewing BIOS Validations"](#) on page 363 for details.
- Export BIOS validation incidents; see ["Exporting BIOS Validation Results"](#) on page 366 for details.
- Delete BIOS validation incidents; see ["Deleting BIOS Validation Incidents"](#) on page 367 for details.

- See Also**
- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device](#) on page 162
 - [Service Now Product Health Data Collection Overview](#) on page 254

Configuring BIOS Validation for Verifying BIOS Integrity of a Device

By configuring BIOS validation, you enable Service Now to collect data from a device running Junos OS for verifying BIOS integrity of the device. If you are configuring BIOS validation for the first time on a device 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 on a device for verifying BIOS integrity:

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

The Service Now Devices page appears.

2. Select a device on which you want to configure BIOS validation.

3. From the Actions list, 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 28: Configure BIOS Validation Dialog Box

4. Perform one of the following tasks:

- If the device is AI-Scripts enabled (that is, AI-Scripts is installed on the 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
- 5. 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.
- 6. (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.
- 7. Click **Submit** to configure BIOS validation or **Cancel** to cancel the configuration.

When you click Submit, Service Now creates a job is created and the Job ID is displayed on the Job Status dialog box.
- 8. 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.

See Also • [AI-Scripts Overview on page 35](#)

Event Profiles and AI-Scripts

- [Service Now Event Profiles Overview on page 165](#)
- [Adding an Event Profile to Junos Space Service Now on page 170](#)
- [Cloning an Event Profile on page 174](#)
- [Importing Event Profiles into Junos Space Service Now in XML Format on page 178](#)
- [Exporting Event Profiles from Junos Space Service Now in XML Format on page 180](#)
- [Deleting Event Profiles from Junos Space Service Now on page 182](#)
- [Viewing an Event Profile on page 182](#)
- [Pushing an Event Profile to Devices on page 183](#)
- [Displaying Devices Associated with an Event Profile on page 186](#)

- [Setting an Event Profile as the Default Event Profile in Junos Space Service Now on page 187](#)
- [Exporting Events Data in Excel Format on page 188](#)
- [Adding a Script Bundle to Junos Space Service Now on page 188](#)
- [Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now on page 189](#)
- [Deleting a Script Bundle from Junos Space Service Now on page 190](#)

Service Now Event Profiles Overview

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

Juniper Networks ships the latest AI-Scripts bundle with Service Now and hence when you install Service Now, the latest AI-Scripts bundle is displayed on the Script Bundles page (**Administration > Event Profiles > Script Bundles**). 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 188](#)).

Service Now also has a default event profile that is associated with the default AI-Scripts bundle. For new Service Now installations or upgrades, Service Now associates the default event profile with the AI-Scripts bundle shipped with Service Now.

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. Service Now uses the default Scripts bundle to create a new event profile and selects the default event profile while installing an event profile on devices.



NOTE: Read the KB article, <https://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. You can clone an event profile to create a new event profile by modifying a few attributes of 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 device.

The priority of event policies in an event profile determine the priority shown in the JMBs generated for a Service Now event. Service Now allows 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.

You can view event profiles on the Event Profiles page (**Administration > Event Profiles**) as shown in [Figure 29 on page 166](#). [Table 17 on page 166](#) lists the information displayed on

the Event Profiles page The default event profile is indicated by a unique icon. In [Figure 29 on page 166](#), Base_Profile_3_7R1_2 is the default event profile.

Figure 29: 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

[Table 17 on page 166](#) lists the parameters of event profiles.

Table 17: Event Profile Parameters

Parameter	Description
Name	Name of the event profile
Description	Description of the event profile
AI-Scripts Version	Version of AI-Scripts used to created the event profile
Created By	User who created the event profile
Created	Date and time when the event profile was created
Events Included	Number of events from the AI-Scripts bundle included in the event profile
Events Excluded	Number of events from the AI-Scripts bundle not included in the event profile
Total Events in Script Bundle	Number of events in the AI-Scripts bundle using which the event profile was created
Events with No Incidents	Number of events for which incidents have not been created
Total Incidents	Number of incidents that are created by using the event profile
Associated Devices	Number of devices on which the event policy is installed
Domain	Domain to which the event policy is assigned

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.

Starting in Service Now Release 15.1R1, 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, a static

AI-Scripts configuration is pushed and committed on the device. The static configuration, once committed on the device, is used during successive installation or upgrade of AI-Scripts. This eliminates 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 30 on page 168](#)) 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 when you install or upgrade and subsequently commit AI-Scripts, clear this check box.

Figure 30: Install Event Profile Page

Install Event Profile

Add to Device Group: Default for Prod_Org

Use Profile: EventProfileREST

Commit Comment: Commit Issued by Service Now.

☐ 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](#)

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, you must manually push the static AI-Scripts configuration and execute the `/var/db/scripts/op/ais-param-set.slax` file on the device.

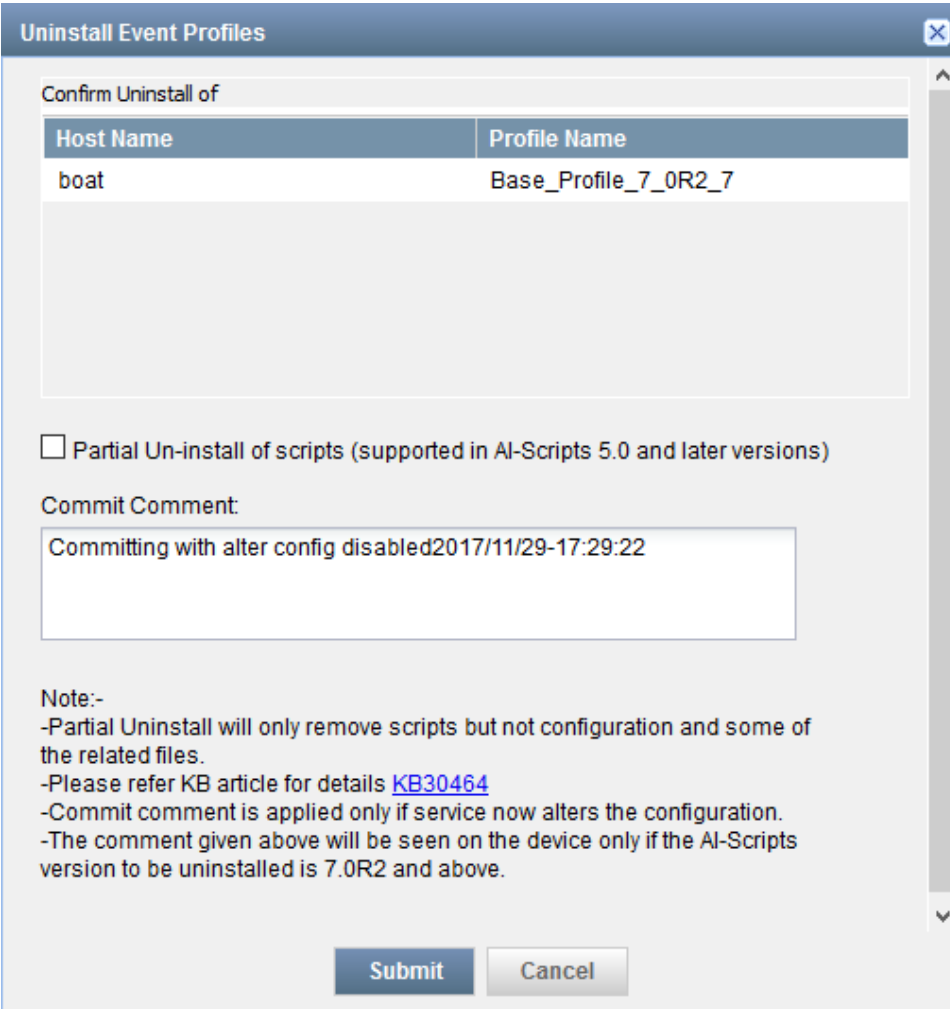
- When you install or upgrade AI scripts releases earlier than Release 5.0 on a device by using Service Now Release 15.1 or later, you must manually push the static AI-Scripts configuration to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable 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 124.

- The **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** check box on the Uninstall Event Profiles dialog box, as shown in [Figure 31 on page 169](#), when selected, provides an option to uninstall AI-Scripts from a device 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 31: Uninstall Event Profile Dialog Box



The dialog box is titled "Uninstall Event Profiles" and contains the following elements:

- Confirm Uninstall of:** A table with two columns: "Host Name" and "Profile Name".

Host Name	Profile Name
boat	Base_Profile_7_0R2_7
- ☐ Partial Un-install of scripts (supported in AI-Scripts 5.0 and later versions)
- Commit Comment:** A text area containing the text: "Committing with alter config disabled2017/11/29-17:29:22"
- Note:-**
 - Partial Uninstall will only remove scripts but not configuration and some of the related files.
 - Please refer KB article for details [KB30464](#)
 - Commit comment is applied only if service now alters the configuration.
 - The comment given above will be seen on the device only if the AI-Scripts version to be uninstalled is 7.0R2 and above.
- Buttons:** "Submit" and "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, you must delete the AI-Scripts configuration on the device by executing the `/var/db/scripts/remove-jais.slax` script 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 128.

Associated Actions

You can perform the following actions related to event profiles:

- Add an event profile to Service Now; see [“Adding an Event Profile to Junos Space Service Now” on page 170](#) for details.
- Push an event profile to devices; see [“Installing an Event Profile on a Device by Using Service Now” on page 124](#) for details.
- View devices associated with an event profile; see [“Displaying Devices Associated with an Event Profile” on page 186](#) 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 187](#) for details.
- Import an event profile in XML format; see [“Importing Event Profiles into Junos Space Service Now in XML Format” on page 178](#) for details.
- Export events data to Excel format; see [“Exporting Events Data in Excel Format” on page 188](#) for details.
- Export an event profile in XML format; see [“Exporting Event Profiles from Junos Space Service Now in XML Format” on page 180](#).
- Clone an event profile; see [“Cloning an Event Profile” on page 174](#) for details.
- Delete event profiles; see [“Deleting Event Profiles from Junos Space Service Now” on page 182](#) for details.
- Add script bundles; see [“Adding a Script Bundle to Junos Space Service Now” on page 188](#) for details .

- See Also**
- [AI-Scripts Overview on page 35](#)
 - [Service Now Devices Overview on page 117](#)
 - [Service Now Incidents Overview on page 302](#)

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. By 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 another AI-Scripts bundle (see [“Adding a Script Bundle to Junos Space Service Now” on page 188](#)).

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 32 on page 171](#).

Figure 32: 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_RTLOAD_FAIL	Software Failure	Initialization error	Medium	View KB	No
<input checked="" type="checkbox"/> CONNECTION_CRAFTO_FAIL	Software Failure	Initialization error	Medium	View KB	No
<input checked="" type="checkbox"/> CONNECTION_CHASSISID_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)					

Page 1 of 1

Displaying 1 - 100 of 435

Submit

Cancel

For a description of the fields displayed on this page, see [Table 18 on page 171](#).

Table 18: Add Event Profile Page Field Descriptions

Field	Description
Profile Name	<p>Enter a name of the event profile.</p> <p>The name can contain alphanumeric characters, underscore, hyphens and space. The maximum number of characters allowed is 255.</p>
Description	<p>Enter a description for the event profile.</p> <p>The maximum number of characters allowed is 255.</p>
Script Bundle	<p>Lists the AI-Scripts bundles that are available in Service Now. This consists of the default AI-Scripts bundle that is available with Service Now and the ones that you upload.</p>
Find Events	<p>Specify an event from the list to filter the displayed list of events</p>
Show Selected Events	<p>Shows all the events that you have selected.</p>
Description of the columns in the Add Event Profiles page	
Event Synopsis	<p>Name used to identify the event script.</p>
Type	<p>Type of event that triggers the event script:</p> <ul style="list-style-type: none">• Hardware failure• Software failure• Resource Exhaustion

Table 18: Add Event Profile Page Field Descriptions (continued)

Field	Description
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. If you want to add a new script bundle and use the new script bundle to create an event profile, click **Add Script Bundle**. See [“Adding a Script Bundle to Junos Space Service Now” on page 188](#) for details about adding a new script bundle to Service Now.

By default, the script bundle that is set as the default is automatically selected for installing the event profile. You can modify this selection if required.
6. (Optional) To search for specific events to be included in the event profile, 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. On the Save Event Profile dialog box, 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. An icon (!) appears on the left-side of the row of a device on which the selected events in the event profile are likely to occur.

Figure 33: 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
<input checked="" type="checkbox"/> (!)	ex-2200-sn3	CW0210403356	EX2200-24T-4G	12.2R3.5
				Click

- (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
- (Optional) To view a device's exposure to known issues, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated with the respective device.
- Click **Return to Potential Exposure** to continue.
- Click **Continue**.
A confirmation dialog box appears displaying the final list of devices on which you want to install the selected event profile.
You can remove devices from the list by clearing the check boxes of the devices you want to remove.
- Click **Install**.
The event profile is installed on the selected devices, 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 183 .
Return to the Profiles Page	The event profile installation task is canceled, and the Event Profiles page appears.

- See Also**
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
 - [Service Now Event Profiles Overview on page 165](#)

Cloning an Event Profile

Junos Space Service Now provides the Clone option in the Actions list of the Event Profiles page to clone an existing event profile and modify its priority to create another event profile. When you clone an event profile, Service Now provides a default name by appending the name of the original event profile with *Copy of*. You can edit this name.



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

To clone an event profile:

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

The **Clone Event Profile** page appears.
3. (Optional) In the **Profile Name**, edit the profile name.

By default, Service Now populates the name of the event profile as a Copy of *event profile* from which the new event profile is being cloned.
4. (Optional) In the **Description** text field, enter a description for the cloned event profile.
5. (Optional) From the **Script Bundle** list, select a script bundle from which to create the cloned event profile..

A **Show difference** button appears.
6. (Optional) Click the **Show difference** button to view the differences in the events between the original script bundle and the newly selected script bundle.

The Event Difference Display dialog box displays the events that are new and deprecated in the newly selected script bundle in comparison with the script bundle used in the original event profile.

After viewing the differences, close the Event difference display dialog box to return to the Clone Event Profile page.
7. (Optional) To search for specific events, enter the name of the event in the **Find Events** search field.

8. (Optional) Click **Priority** for each event to modify the event priority. The values are:

1. Low
2. Medium
3. High
4. Critical

9. Click **Submit**. The event profile is created and the **Save Event Profile** dialog box appears.

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

Link	Result
Apply this profile to original set of devices	

Link	Result
	<p>When you click this link, the Select Devices to Install Profile section appears on the Clone Event Profile page..</p> <p>In this page, specify the following options for installing the profile on the devices:</p> <ul style="list-style-type: none"> Specify the devices on which you want to install the event profiles by selecting the respective check box present on the left side of the row. To specify all the listed devices, select the check box present next to Organization column heading. 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. This check box is cleared by default. NOTE: If you select this check box, roll back to this version of the AI-Scripts bundle is not possible in future. 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.. 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: <ul style="list-style-type: none"> 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 <code>/var/db/scripts/op/ais-param-set.slax</code> 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. 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. An (!) icon present on the left-side of a device row indicates that the device is susceptible to events in the event profile.</p> <p>On 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

Link	Result
	selected devices.
Apply this profile to devices manually	<p>When you click this link, the Push to Devices page appears.</p> <p>On this page, you can select Service Now devices and install event profiles on the selected devices.</p> <p>For information about installing event profiles on devices, see “Pushing an Event Profile to Devices” on page 183.</p>
Return to the Profiles Page	<p>When you click this link, Service Now cancels the installation of event profile on devices and displays the Event Profiles page.</p> <p>The cloned event profile is listed on the Event Profiles page.</p>

- See Also**
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
 - [Service Now Event Profiles Overview on page 165](#)

Importing Event Profiles into Junos Space Service Now in XML Format

Junos Space Service Now provides the Import Event Profiles option in the Actions list of the Event Profiles page to import event profiles in the XML format to Service Now. You can import only one XML file at a time. To import multiple event profiles at the same time, include all the event profiles 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 importing into Service Now:

```
<eventProfiles>
  <eventProfile>
    <profileInformation>
      <profileName>Base_profile</profileName>
      <description>Base Profile for Bundle 4.1R1.1</description>
      <scriptBundleVersion>6.0R1.0</ scriptBundleVersion >
      <scriptBundleFileName>jais-6.0R1-signed.tar</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>
      </script>
    </scripts>
  </eventProfile>
</eventProfiles>
```

```

        <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>
<eventProfile>
  ...
  ...
  ...
</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 34 on page 179](#).

Figure 34: View Event Profiles Page

2. Click **Browse** to browse for the event profile file and click **Upload**.

Service Now imports the event profile file and lists the imported event profiles on the Event Profiles page.

See Also • [Service Now Event Profiles Overview on page 165](#)

Exporting Event Profiles from Junos Space Service Now in XML Format

Junos Space Service Now provides the Export All Profiles and Export Selected Profiles options on the Actions list of the Event Profiles page to export event profiles in the XML format. Service Now includes all event profiles to be exported in a single XML file.

The following sample is an example of an event profile exported by Service Now:

```
<eventProfiles>
  <eventProfile>
    <profileInformation>
      <profileName>Base_profile</profileName>
      <description>Base Profile for Bundle 4.1R1.1</description>
      <scriptBundleVersion>6.0RR1.1</scriptBundleVersion>
      <scriptBundleFileName>jais-6.0R1-signed.tar</scriptBundleFileName>
      <creationTime>[In seconds]</creationTime>
      <userCreated>super</userCreated>
      <eventsIncluded>440</eventsIncluded>
      <eventsExcluded>0</eventsExcluded>
      <deviceInstalled>2</deviceInstalled>
    </profileInformation>

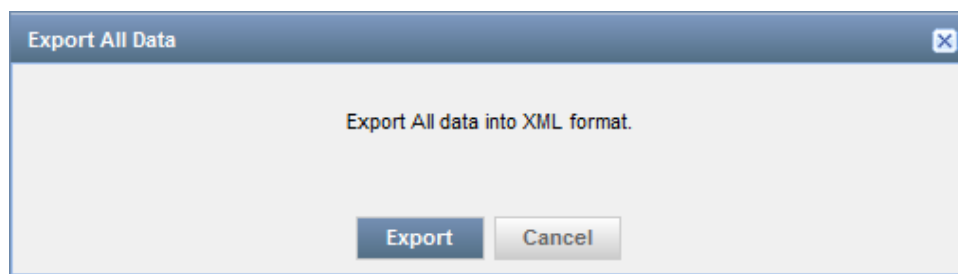
    <scripts>
      <script>
        <scriptId>47</scriptId>
        <eventId>ACCT_MALLOC_FAILURE</eventId>
        <scriptName>ACCT_MALLOC_FAILURE.slax</scriptName>
        <processId>PFED</processId>
        <eventTypeGroup>Resource Exhaustion</eventTypeGroup>
        <eventType>Memory Consumption</eventType>
        <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 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 list. Alternatively, right-click on an event profile and select **Export All Profiles**.

The Export All Data dialog box appears as shown in [Figure 35 on page 181](#).

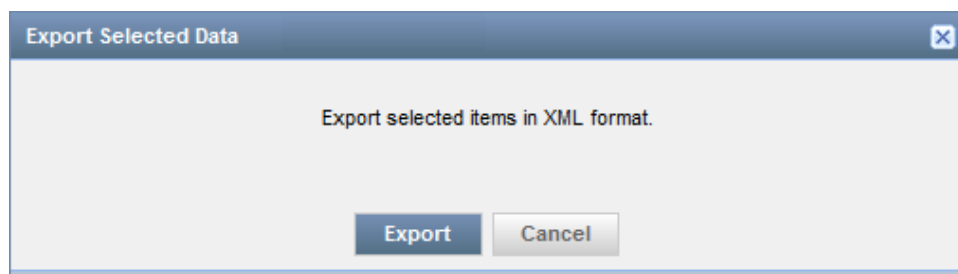
Figure 35: Export All Data Dialog Box



- To export selected event profiles, click the event profiles that you want to export and select **Export Selected Profiles** from the Actions list. 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 36 on page 181](#).

Figure 36: 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.

- See Also**
- [Service Now Event Profiles Overview on page 165](#)
 - [Importing Event Profiles into Junos Space Service Now in XML Format on page 178](#)

Deleting Event Profiles from Junos Space Service Now

Junos Space Service Now provides the Delete option in the Actions list of the Event Profiles page to delete event profiles. You can delete an event profile only if it is not associated with a device.

When you delete a default event profile, Service Now sets the most recently created event profile as the default event profile.

To delete event profiles:

1. From the Service Now navigation tree, select **Administration > Event Profiles**.
The Event Profiles page appears.
2. Select one or more 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.
Service Now deletes the selected event profiles and removes the deleted event profiles from the Event Profiles page.

See Also • [Displaying Devices Associated with an Event Profile on page 186](#)

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.

See Also • [Exporting Events Data in Excel Format on page 188](#)

- [Cloning an Event Profile on page 174](#)
- [Pushing an Event Profile to Devices on page 183](#)

Pushing an Event Profile to Devices

An event profile is a set of event policies that are selected from an AI-Scripts bundle. When you push an event profile onto Juniper Networks devices, these event policies are installed on the devices. The event policies automatically detect and report problems (incident) that occur on the device and also provide monitoring information.

Junos Space 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 on the devices of end customers.
- For information about behavior of AI-Scripts when installed on specific product families, see <https://kb.juniper.net/InfoCenter/index?page=content&id=KB29188>.

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** page appears (see [Figure 37 on page 184](#)).

Figure 37: 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 | 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 1107 1108 1109 1110 | 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 | 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 | 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 | 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 | 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 | 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 | 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 | 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 | 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 | 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 | 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 | 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 | 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 | 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 | 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 | 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 | 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 | 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 | 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 | 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 | 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 | 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 | 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 | 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 | 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 | 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 | 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 | 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 | 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 | 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 | 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 | 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 | 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 | 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 | 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 | 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 | 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 | 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 | 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 | 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 | 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 | 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 | 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 | 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 | 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 | 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 | 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 | 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 | 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 | 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 | 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 | 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 | 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 | 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 | 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 | 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 | 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 | 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 | 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 | 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 | 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 | 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 | 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 | 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 | 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 | 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 | 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 | 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 | 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 | 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 | 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 | 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 | 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 | 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 | 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 | 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 | 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 | 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 | 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 | 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 | 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 | 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 | 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 | 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 | 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 | 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 | 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 | 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 | 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 | 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 | 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 | 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 | 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 | 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 | 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 | 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 | 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 | 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 | 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 | 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 | 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 | 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 | 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 | 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 | 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 | 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 | 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 | 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 | 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 | 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 | 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 | 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 | 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 | 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 | 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 | 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 | 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 | 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 | 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 | 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 | 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 | 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 | 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 | 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 | 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 | 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 | 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 | 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 | 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 | 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 | 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 | 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 | 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 | 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 | 2451 2452 2453 2454 2455 2456

**NOTE:**

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

7. (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 when you want to install the event profile in the **Date and time** field.

Service Now installs the event profile at the configured date and time.

8. Click **Submit**.

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

Figure 38: Potential Exposure to Known Issues Page

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

9. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.

10. (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.

11. Click **Return to Potential Exposure** to continue.

12. 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.

13. 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.

14. Click **OK**.

The View Event Profiles page appears.

- See Also**
- [Service Now Event Profiles Overview on page 165](#)
 - [Viewing Exposure for a Device on page 132](#)

Displaying Devices Associated with an Event Profile

Junos Space Service Now provides the Show Associated Devices option in the Actions list of the Event Profiles page to view devices that are associated with a specific event profile. This task is disabled when you select an event profile that is not associated with 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.

- See Also**
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
 - [Adding an Event Profile to Junos Space Service Now on page 170](#)

Setting an Event Profile as the Default Event Profile in Junos Space Service Now

Junos Space Service Now provides the Set as Default Profile option in the Actions list of the Event Profiles page 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 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 appears and 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 an event profile. The default event profile (for example, Base_Profile_3_7R1_2 in [Figure 39 on page 187](#)) shows the default event profile indicated by the unique icon.

Figure 39: 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

- See Also**
- [Displaying Devices Associated with an Event Profile on page 186](#)
 - [Cloning an Event Profile on page 174](#)
 - [Pushing an Event Profile to Devices on page 183](#)

Exporting Events Data in Excel Format

Junos Space 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.
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. Select **Open with** to open the Excel file or select **Save File** to save the file on your local system.
5. Click **OK**.
The event activity information that appears in the Event Profile Detail dialog box is contained in the following five worksheets in the Excel file:
 - Event Activity(7 days)
 - Event Activity(30 days)
 - Event Activity(365 days)
 - New Active Events
 - Inactive Selected Events

- See Also**
- [Installing an Event Profile on a Device by Using Service Now on page 124](#)
 - [Service Now Event Profiles Overview on page 165](#)

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 on the system running the Service Now application. You need Service Now Administrator privileges to add a script bundle.



NOTE: The script bundle is distributed as a *.tgz file for releases prior to AI-Scripts Release 6.0R1.0. From AI-Scripts Release 6.0R1.0, the script bundle is distributed as a *.tar file.

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 by using this script bundle. See [“Adding an Event Profile to Junos Space Service Now” on page 170](#).

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 40 on page 189](#).

Figure 40: Add Script Bundle Dialog Box

The dialog box titled "Add Script Bundle" contains a text input field labeled "Script Bundle:" followed by a "Browse..." button. Below these 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.

- See Also**
- [AI-Scripts Overview on page 35](#)
 - [Installing an Event Profile on a Device by Using Service Now on page 124](#)

Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now

Junos Space Service Now provides the Set as Default Bundle option in the Actions list of the Script Bundles page 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 policies to be included in 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, Service Now sets the most recently uploaded script bundle as the default script bundle.

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.

- See Also**
- [AI-Scripts Overview on page 35](#)
 - [Installing an Event Profile on a Device by Using Service Now on page 124](#)

Deleting a Script Bundle from Junos Space Service Now

Junos Space Service Now provides the Delete option in the Actions list on the Script Bundles page to delete script bundles.

You cannot delete a script bundle if:

- The script bundle is preloaded with Service Now
- An event profile created by using the script bundle is installed on a device

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 bundles 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 appears and prompts you to confirm the deletion.

3. Click **Delete**.

Service Now deletes the script bundles from the database and returns to the Script Bundles page. The deleted script bundles are no longer listed on the Script Bundles page.

- See Also**
- [AI-Scripts Overview on page 35](#)
 - [Installing an Event Profile on a Device by Using Service Now on page 124](#)

Global Settings

- [Configuring Global Settings on page 191](#)
- [Adding an SNMP Configuration to Service Now on page 194](#)
- [Editing an SNMP Configuration on page 196](#)
- [Managing SNMP Traps on page 196](#)
- [Viewing Proxy Server Settings Configured on the Junos Space Platform on page 197](#)
- [Configuring SFTP Server for Uploading Core Files Generated for Events on page 198](#)
- [Directive File Overview on page 200](#)
- [Viewing the Directive File on page 201](#)
- [Updating the Directive File in Junos Space Service Now on page 202](#)
- [Restoring the Default Directive File on page 204](#)
- [Configuring Advanced Filter Settings on page 205](#)

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.

Starting in Service Now Release 16.1R1, the **Submitted Incident Purge Time (in days)** and **Not Submitted Incident Purge Time (in days)** fields are available on the Global Settings page to define the number of days after which incidents that are submitted to JSS and incidents that are not submitted to JSS can be purged respectively

Starting in Service Now Release 16.1R1, the **Do not auto submit Incident which are older (in days)** is available on the Global Settings page to prevent incidents older than the number of days specified in the field from being submitted to JSS by auto submit policies.

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 41 on page 192](#).

Figure 41: Global Settings Page

The screenshot shows the 'Global Settings' page with the following fields and options:

- Outbound Email Address:**
- Device Snapshot Purge Time (in days):** (dropdown arrow)
- Product Health Data Purge Time (in days):** (dropdown arrow)
- Submitted Incident Purge Time (in days):** (dropdown arrow)
- Not Submitted Incident Purge Time (in days):** (dropdown arrow)
- Device Log File Purge Time (in days):**
- Do not auto submit Incident which are older (in days):**
- Repeat Incident Dampening Period:** (dropdown arrow)
- ☒ Share Service Now Profile Information
- ☒ Collect Log Files
- Connection Status:** OK

At the bottom, there are three buttons: **Save**, **Test Connection**, and **Cancel**.

- Enter values for the global settings as described in [Table 19 on page 192](#).
- Click **Save** to save the global settings and update Service Now or 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 configuring global settings is displayed.

[Table 19 on page 192](#) describes the fields displayed on the Global Settings page.

Table 19: 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)	<p>Number of days device snapshots of a device are stored in the Service Now database before they are deleted</p> <p>0 indicates that device snapshots are never purged.</p>	<ul style="list-style-type: none"> • 0 • 90 • 120 • 180 • 365 	180

Table 19: Global Settings Parameters (continued)

Name	Description	Range/Length	Default
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>0 indicates that the information about PHD is never deleted from the database.</p>	<ul style="list-style-type: none"> • 0 • 30 • 45 • 60 • 90 • 120 • 180 • 365 	30
Submitted Incident Purge Time (in days):	<p>Number of days incidents submitted to JSS are stored in the Service Now database before they are deleted</p> <p>0 indicates incidents submitted to JSS or Service Now partner are never purged.</p>	<ul style="list-style-type: none"> • 0 • 30 • 45 • 60 • 90 • 120 • 180 • 365 	365
Not Submitted Incident Purge Time (in days):	<p>Number of days incidents that are not submitted to JSS are stored in the Service Now database before they are deleted</p> <p>0 indicates incidents that are not submitted to JSS or Service Now partner are never purged.</p>	<ul style="list-style-type: none"> • 0 • 30 • 45 • 60 • 90 • 120 • 180 • 365 	365
Device Log File Purge Time (in days)	Number of days log files collected from devices are stored in the Service Now database before they are deleted.	1 – 365	30
Do not Auto Submit Incident which are older (in days):	Number of days after which incidents are not submitted to JSS by using auto submit policies	1 – 365	3

Table 19: Global Settings Parameters (continued)

Name	Description	Range/Length	Default
Repeat Incident Dampening Period	<p>The time period during which Service Now does not create new incidents on receipt of JMBs for the same event 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 creates an incident only for 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>0 indicates Service Now creates incidents for all JMBs received for the same incident.</p> <p>For information about the Auto Submit Policy, see “Creating an Auto Submit Policy” on page 243.</p>	<ul style="list-style-type: none"> • 0 • Always • 1hr – 12hr • 1 day – 5 days • 10 days • 15 days • 20 days • 25 days • 30 days • 45 days • 60 days • 90 days • 120 days 	0
Share Service Now Profile Information	<p>If this check box is selected, all Service Now-related information is shared with JSS or Service Now partner 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"> • OK • No route to host • Connection refused • The Home Base server is temporarily unable to service your request 	

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Service Now Device Snapshots Overview on page 357](#)[Service Now Product Health Data Collection Overview on page 254](#)
 - [Service Now Product Health Data Collection Overview on page 254](#)

Adding an SNMP Configuration to Service Now

Junos Space Service Now provides the SNMP configuration task to specify a destination for SNMP traps to be sent when a Service Now notification policy is triggered. SNMP traps are sent to the specified 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.

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 server where Service Now SNMP traps are sent.

5. In the **UDP Port** text box, enter the UDP port number.

The default UDP Port number is 162.

6. In the **Community String** text box, 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 SNMP version you want to use from the **Protocol Version** drop-down list.

8. Click **Add**.

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

Loading MIBs

When using a MIB browser or other SNMP trap receivers such as HP OpenView to monitor the devices, the following MIB files must be loaded:

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



NOTE: The `jnx-smi.mib` file must be loaded first.

- See Also**
- [Service Now Notification Policies Overview on page 384](#)
 - [SNMP MIBs Downloads](#)

Editing an SNMP Configuration

An SNMP configuration defines 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 SNMP configuration 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 Configuration page appears.

2. Select the SNMP server configuration that 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.

6. (Optional) To verify, you can view the changes on the SNMP Configurations page.

- See Also**
- [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 used. See [Figure 42 on page 197](#).

An attribute is added to a notification if the check box next to it is selected. To add or remove attributes from notifications, select or clear the check box for an attribute. By default, all attributes for all notifications are selected.

Figure 42: SNMP Trap Attribute Page

Administration > Global Settings > SNMP Configuration > Manage SNMP Traps

SNMP Trap Attributes	
Attribute Name	Notifications
<input checked="" type="checkbox"/> description	New PBN Match, New PBN Arrival, New EOL Match, New Exposure, Service Contract Expiring, New Incident Detected, Case ID Assigned, Case Status Updated, New Intelligence Update, Incident Submitted, Ship-to Address Missing For Device, Switch over enabled for IJMB, Connected Member Device Added/Removed, Partner Certificate Expiry, Partner Certificate Expired, Product Health Data Collection Failure
<input checked="" type="checkbox"/> device	New PBN Arrival, New EOL Match, New Exposure, Service Contract Expiring, Case ID Assigned, Case Status Updated, New Incident Detected, Incident Submitted, Ship-to Address Missing For Device, Switch over enabled for IJMB, Connected Member Device Added/Removed, Product Health Data Collection Failure
<input checked="" 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 checked="" type="checkbox"/> issueDate	New Intelligence Update
<input checked="" type="checkbox"/> caseID	Case ID Assigned, Case Status Updated
<input checked="" type="checkbox"/> hostID	New Incident Detected, Incident Submitted, Case ID Assigned, Case Status Updated, Ship-to Address Missing For Device
<input checked="" type="checkbox"/> serialNumber	Service Contract Expiring, Switch over enabled for IJMB, Connected Member Device Added/Removed
<input checked="" type="checkbox"/> partNumber	Service Contract Expiring
<input checked="" type="checkbox"/> contractAgreementNumber	Service Contract Expiring
<input checked="" type="checkbox"/> contractAgreementStatus	Service Contract Expiring
<input checked="" type="checkbox"/> contractSKU	Service Contract Expiring
<input checked="" type="checkbox"/> contractSKUType	Service Contract Expiring
<input checked="" type="checkbox"/> contractStartDate	Service Contract Expiring
<input checked="" type="checkbox"/> contractEndDate	Service Contract Expiring
<input checked="" type="checkbox"/> product	New Exposure, Switch over enabled for IJMB

Page 1 of 2 | Displaying 1 - 30 of 32



NOTE:

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

See Also • [SNMP MIBs Downloads](#)

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** on the Junos Space Network Management Platform navigation tree. The Proxy Server page lists the proxy servers configured on Network Management Platform.

- See Also**
- [Configuring Proxy Server Settings in Network Management Platform](#)
 - [Configuring Global Settings on page 191](#)
 - [Adding an SNMP Configuration to Service Now on page 194](#)

Configuring SFTP Server for Uploading Core Files Generated for Events



NOTE: From starting of the year 2018, Juniper Networks does not support uploading core files to an FTP server; you can only upload core files to an SFTP server.

You can configure an SFTP server in Service Now to upload core files that are generated for an event or related to an event. A core file is generated when a fault occurs on a device. You can upload specific core files either when an incident is submitted to Juniper Support Systems (JSS) or Service Now partner to open a case for the event or after the case is opened.

You can configure an SFTP server only if Service Now is operating in the Partner Proxy, Direct, or Demo mode. In the End Customer mode, Service Now uses SFTP server configured by the Service Now partner to upload core files. The core files are uploaded to the SFTP server and associated with the case number assigned to the incident by the partner. The Service Now partner uploads the core files to JSS where it is associated with the case number provided by JSS.

You cannot configure SFTP server to upload core files in an Offline mode.

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 as shown in [Figure 43 on page 199](#).

Figure 43: Core File Upload Configuration Page

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

The available options are:

- **Disabled-Core Files uploaded manually:** If you select this option, Service Now does not upload core files to the FTP server. You have to manually upload the core files to the SFTP server.
- **Secure FTP upload through Service Now:** If you select this option, Service Now uploads the core files to the SFTP server after downloading the core files from a device.

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 connectivity of Service Now with the SFTP server.

The **SFTP Server Status** field displays **Success** if the Service Now is able to connect to the SFTP server.

See Also • [Updating Core File Upload Configuration for an End Customer on page 110](#)

Directive File Overview

Junos Space Service Now creates off-box Juniper Message Bundle (JMB) by using a directive file (**directive.rc**). The directive file stores a list of devices for which Service Now can generate JMBs without using the AI-Scripts (off-box JMBs) installed on the devices.

Service Now provides a default directive file. The directive file is updated automatically to include support for new devices using updates from Juniper Support Systems (JSS). Starting in Service Now Release 16.1R1, Service Now provides options to manage the directive file so that off-box JMBs can be generated for devices newly supported by Service Now.



NOTE: Service Now executes the RSI brief command on devices running subscriber management services instead of the normal RSI command to avoid impacting performance of device CPU.

For Service Now operating in Offline mode, Juniper Networks provides the directive file by e-mail, which can be manually uploaded to Service Now. Service Now operating in End Customer mode receives updates, if any, from the Service Now partner once every 24 hours and the directive file is updated. Service Now does not verify the contents of the directive file that you upload, but only validates the version of the directive file. Therefore, we recommend that you do not modify the directive file.

You can view the directive file on the Directive File page (**Administration > Global Settings > Directive File**) as shown in [Figure 44 on page 200](#).

Figure 44: Directive File Page

Name	Version	Updated On	Updated By	Remarks	View	Upload
DirectiveFile.rc	2.2	Jul 14, 2016 12:51:00 PM IST	Service Now		View/Modify	Upload

The Directive File page displays the following details:

- Name—name of the directive file
- Version—version of the directive file
- Updated On—date and time the directive file was last updated

- Updated by—entity that updated the directive file; the value is Service Now if the file is automatically updated by Service Now; otherwise, the username of the user who uploaded the directive file is listed
- Remarks—any remarks about the directive file
- View—link to view or modify the directive file
- Upload—link to upload a directive file

You can perform the following tasks from the Directive Files page:

- Update the directive file with the latest file available in JSS; see [“Updating the Directive File in Junos Space Service Now” on page 202](#) for details
- Restore the directive file shipped with Service Now; see [“Restoring the Default Directive File” on page 204](#) for details

See Also • [Generating an On-Demand Incident on page 133](#)

Viewing the Directive File

You can view the directive file used by Junos Space Service Now for generating off-box Juniper Message Bundles (JMBs) in the Directive File task.

To view the directive file

- From the Service Now navigation tree, select **Administration > Global Settings > Directive File**.

The Directive File page appears as shown in [Figure 45 on page 201](#).

Figure 45: Directive File Page

Name	Version	Updated On	Updated By	Remarks	View	Upload
DirectiveFile.rc	2.2	Jul 14, 2016 12:51:00 PM IST	Service Now		View	Upload

The Directive File page displays the following details:

- Name—name of the directive file
- Version—version of the directive file
- Updated On—date and time the directive file was last updated
- Updated by—entity that updated the directive file; the value is Service Now if the file is automatically updated by Service Now; otherwise, the username of the user who uploaded the directive file is listed

- Remarks—any remarks about the directive file
- View—link to view or modify the directive file
- Upload—link to upload a directive file

- See Also**
- [Directive File Overview on page 200](#)
 - [Updating the Directive File in Junos Space Service Now on page 202](#)
 - [Restoring the Default Directive File on page 204](#)

Updating the Directive File in Junos Space Service Now



NOTE: Service Now does not validate the contents of the directive file that you upload. Therefore, we recommend that you do not modify the directive file. If you want changes to the directive file, contact Juniper Networks for assistance.

Changes to a directive file are tracked by version number of the directive file. Service Now checks Juniper Support Systems (JSS) (in Direct or Partner Proxy mode) or the Service Now partner (in case of End Customer) once every 24 hours for updates to the directive file. Any change to the directive file is indicated by a change in the version number. If the version number of the directive file in JSS or Service Now partner is higher than the version number of the directive file in Service Now, Service Now fetches the directive file from JSS or Service Now partner and replaces the file in the Service Now database with the fetched file. To view the details and the content of the updated file on the Directive File page, see [“Directive File Overview” on page 200](#).

You can also use the Refresh option provided on the Directive file dialog box to check for updates to the directive file in JSS or Service Now partner and fetch the updated directive file.



NOTE: Starting Service Now Release 17.1R1, Update Directive File From Juniper Support System check box available in the Advanced Settings task of the Global Settings menu provides an option to avoid updating the directive file in Service Now automatically when a newer version of the directive file is available in JSS.

To use the Refresh option:

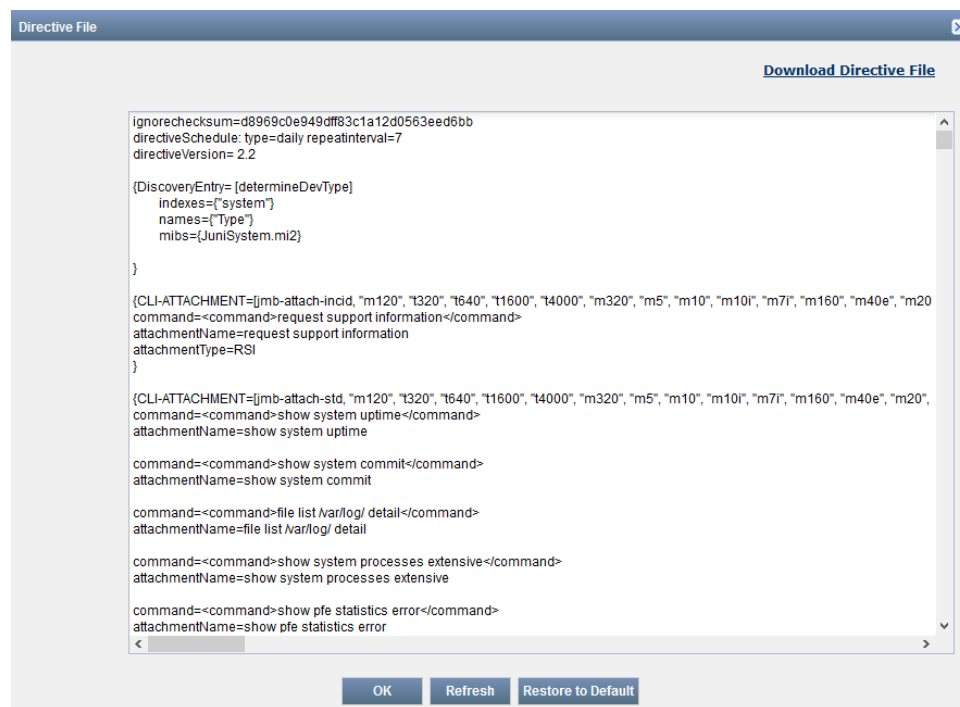
1. From the Service Now navigation tree, select **Administration > Global Settings > Directive File**.

The Directive File page appears.

2. Click the **View/Modify** link in the View column.

The Directive File dialog box appears as shown in [Figure 46 on page 203](#).

Figure 46: Directive File Dialog Box



3. Click the **Refresh** button.

Service Now replaces the current directive file with the latest file from JSS or Service Now partner.

Check the last updated date and time in the Updated On column and the version number in the Version column of the Directive File page to confirm that the directive file is updated. The directive file is updated only if the version of the file in JSS or Service Now partner is higher than that of the file in the Service Now database.

For Service Now operating in Offline mode, Juniper Networks provides the directive file. The directive file must be manually uploaded to Service Now.

Before you begin, store the directive file you receive on your local system.

To manually upload a directive file to Service Now:

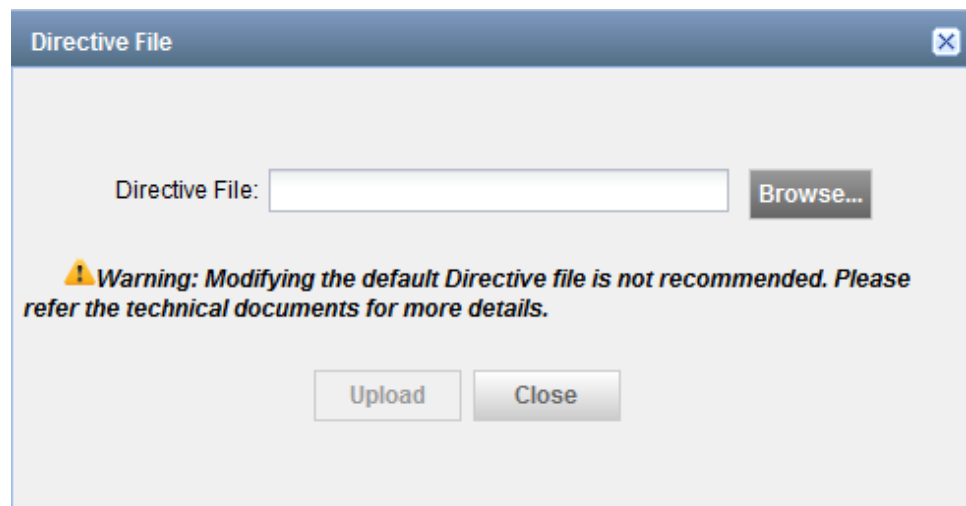
1. From the Service Now navigation tree, select **Administration > Global Settings > Directive File**.

The Directive File dialog box appears.

2. Click the **Upload** link in the Upload column.

The Directive File dialog box appears as shown in [Figure 47 on page 204](#).

Figure 47: Directive File Upload Dialog Box



3. Click the **Browse** button to browse for the received directive file.
4. Click **Upload** to upload the directive file.
The received directive file is uploaded to Service Now.
5. Confirm that the received file is uploaded by checking the version number displayed on the Directive File page. The version number should reflect the version number on the directive file received from Juniper Networks or the Service Now partner.

Restoring the Default Directive File

Junos Space Service Now provides the Restore option to replace an updated or modified directive file with the default directive file shipped with Service Now.

To restore the default directive file shipped with Service Now:

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

The Directive File page appears.

2. Click the **View/Modify** link in the Modify column.

The Directive File dialog box appears.

3. Click the **Restore to Default** button.

Service now restores the current file with the default directive file.

Configuring Advanced Filter Settings

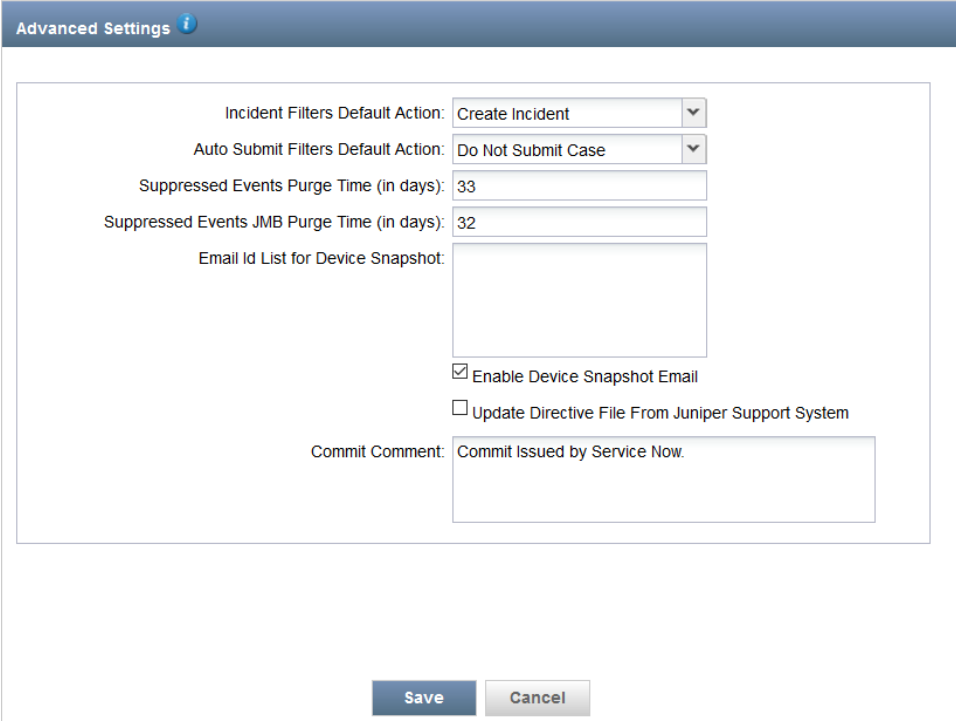
Advanced filter settings define the action that Service Now should take when a JMB or an incident does not match any of the defined incident or auto submit filters. You can define the advanced filter settings in the Global settings task.

To define advanced filter settings:

1. In the Service Now navigation tree, click **Administration > Global Settings > Advanced Settings**.

The Advanced Settings page appears as shown in [Figure 48 on page 205](#).

Figure 48: Advanced Settings Page



Advanced Settings

Incident Filters Default Action: Create Incident

Auto Submit Filters Default Action: Do Not Submit Case

Suppressed Events Purge Time (in days): 33

Suppressed Events JMB Purge Time (in days): 32

Email Id List for Device Snapshot:

☒ Enable Device Snapshot Email

☐ Update Directive File From Juniper Support System

Commit Comment: Commit Issued by Service Now.

Save Cancel

2. On the Advanced Settings page, configure values for parameters as follows:
 - Select a default action for incident filters in the **Incident Filters Default Action** drop-down list—Create Incident, Do not Create Incident.
 - Select a default action for auto submit filters in the **Auto Submit Filters Default Action** drop-down list—Submit Case, Do Not Submit Case.
 - Enter the number of days suppressed events can be stored in the Service Now database before they are deleted in the **Suppressed Events Purge Time (in days)** text box.



NOTE: Whenever the suppressed events are purged or deleted, the associated JMBs are also purged or deleted. However, if suppressed JMBs are deleted, the suppressed events are not deleted.

- Enter the number of days suppressed JMBs can be stored in the Service Now database before they are deleted in the **Suppressed Events JMB Purge Time (in days)** text box.

- In the **Email Id List for Device Snapshot** field, enter the list of e-mail IDs of users to whom you want to send device snapshots by e-mail.

If you do not configure any e-mail IDs, device snapshots are sent by e-mail only to the Super user. If you configure e-mail IDs, then device snapshots are sent by e-mail to only the configured e-mail IDs and not to the Super user.

- (Optional) Clear the **Enable Device Snapshot Email** check box to disable sending device snapshots as an email attachment to users.

By default, this check box is selected and e-mail with device snapshots as attachment is sent to all e-mail IDs configured in the Email Id List for Device Snapshot text field or to the Super user if no e-mail ID is provided.

- (Optional) Clear the **Update Directive File From Juniper Support System** check box to avoid service Now from automatically updating the directive file..

By default, the Update Directive File From Juniper Support System check box is selected and Service Now automatically updates the directive file when a newer version of the file is available in JSS or Service Now partner (in case of End Customer mode).

3. (Optional) Enter a generic comment while installing or uninstalling event profiles in the **Commit Comment** text box.

The comment you enter in this text box appears as the default comment in the **Commit Comment** text box on the Install Event Profile and Uninstall Event Profile pages (**Administration > Service Now Devices > Device Operations**). If you do not add a comment, Service Now adds the following default comment: Commit Issued by Service Now.

This comment is also used as the commit comment for the AI-Scripts configuration while uninstalling AI-Scripts configuration from a device before deleting the device from Service Now.

4. Click **Save** to save the changes.

Service Now displays a confirmation message indicating that the changes are successfully saved.

Incident Filters

- [Service Now Incident Filters Overview on page 207](#)
- [Viewing Incident Filters Configured on Junos Space Service Now on page 209](#)
- [Creating Incident Filters on page 210](#)
- [Modifying an Incident Filter on page 214](#)
- [Deleting Incident Filters on page 216](#)
- [Exporting Incident Filters on page 218](#)
- [Reordering Incident Filters on page 219](#)
- [Enabling Incident Filters on page 220](#)
- [Disabling Incident Filters on page 221](#)

Service Now Incident Filters Overview

Junos Space Service Now receives a Juniper Message Bundle (JMB) from a device, when an event occurs on the device, and creates an incident for the event. Starting in Service Now Release 17.1R1, incident filters provide you the option to select JMBs for which incidents can be created at a granular level. For information about incidents, see [“Service Now Incidents Overview” on page 302](#).

You can use incident filters for the following purposes:

- Define the JMBs for which incidents should be created
- Define the JMBs for which incidents should not be created

Service Now displays all the configured incident filters on the Incident Filters page (**Administration > Incident Filters**).

When a JMB is received, Service Now applies the incident filter having the highest order, that is order 1, to it. If the JMB matches the term criteria of the filter, Service Now either creates an incident for the JMB or lists the JMB under Suppressed Events depending on the action defined in the filter. If the JMB does not match the term criteria of the filter with order 1, Service Now applies the incident filter with order 2. If the JMB matches the term criteria of the filter with order 2, Service Now creates an incident or lists the JMB under Suppressed Events depending on the action defined in the filter.

Service Now applies all the configured filters in the decreasing order till a match is found and performs the action specified in the matching filter. If no filter matches the JMB, Service Now performs the action defined in the Advanced Filter Settings under Global Settings.

Service Now provides options to define a basic filter or an advanced filter. You can also import filters to Service Now in XML format.

Basic filters filter JMBs based on attributes such as event synopsis, platform, event type and so on by using the *and* and *or* predefined computational logic. Advanced filters use

Perl script to define the filtering logic and thereby provide the flexibility to define your own filtering logic.

Starting with Service Now Release 17.2R1, you can use in-built or custom Perl modules in advanced incident filters. For example, you can use custom Perl module for implementing a filtering logic and use that filtering logic across multiple advanced incident filters.

For using a Perl module, you can store the Perl module (*.pm) in any desired location in the Junos Space server and ensure that the Perl module files have read and executable permissions and are accessible by the advanced filters.

Starting with Service Now 17.2R1 release, incident filters are stored at the `/var/cache/jboss/sn/advanced_filter` location of the Junos Space server.



NOTE: The Perl module in-built in Service Now includes an API, `getExistingIncidents()`, for getting information about the latest 20 incidents. The API is included in the `FilterUtilV1.pm` file stored in `/var/cache/jboss/SN/AdvancedFilters`. For more information, see [“Sample Perl Script for Incident and Auto Submit Filters” on page 457](#).



NOTE:

- Incident filters cannot be applied to on-demand JMBs, BIOS JMBs, AIS Health Report JMBs, and Product Health Data JMBs
- In a Service Now partner, incident filters cannot be applied to JMBs received from a Service Now end customer.
- There is no limit on the number of filters that can be created. However, a large number of incident filters impacts the performance of Service Now when creating incidents.

Associated Actions

You can perform the following actions related to incident filters:

- View incident filters; see [“Viewing Incident Filters Configured on Junos Space Service Now” on page 209](#) for details.
- Create incident filters; see [“Creating Incident Filters” on page 210](#) for details.
- Modify incident filters; see [“Modifying an Incident Filter” on page 214](#) for details.
- Export incident filters; see [“Exporting Incident Filters” on page 218](#) for details.
- Reorder incident filters; see [“Reordering Incident Filters” on page 219](#) for details.
- Enable incident filters; see [“Enabling Incident Filters” on page 220](#) for details.
- Disable incident filters; see [“Disabling Incident Filters” on page 221](#) details.
- Delete incident filters to a domain; see [“Deleting Incident Filters” on page 216](#) for details.

- See Also**
- [Service Now Auto Submit Filters Overview on page 222](#)
 - [Service Now Incidents Overview on page 302](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Service Now Suppressed Events Overview on page 380](#)

Viewing Incident Filters Configured on Junos Space Service Now

You can view incident filters that are configured on Junos Space Service Now on the Incident Filters page.

To view incident filters configured on Service Now, in the Service Now navigation tree, click **Administration > Incident Filters**. The Incident Filters page appears as shown in [Figure 49 on page 209](#).

Figure 49: Incident Filters Page

Name	Type	Action	Created By	Status	Created Time	Updated Time	Order
Test	Advanced	Do not create Incident	super	Enabled	May 19, 2017 2:28:57 PM IST	May 19, 2017 2:28:57 PM IST	3
test_basic_filter_After	Basic	Do not create Incident	super	Enabled	May 17, 2017 6:53:50 PM IST	May 19, 2017 3:43:53 PM IST	2

[Table 20 on page 209](#) lists the information about Incident Filters displayed on the Incident Filters page.

Table 20: Fields in Incident Filters Page

Column	Description
Name	Name of the incident filter
Type	Type of filter: Basic or Advanced
Action	Action to be taken on a JMB when the JMB matches the conditions of the filter term: Create Incident or Do not create Incident
Created By	User who created the filter
Status	Status of the filter: Enabled or Disabled
Created Time	Date and time the filter was created
Updated Time	Date and time the filter was last updated
Order	Order in which the filters are applied to JMBs. By default, Service Now lists the filter with the highest order first. See “Reordering Incident Filters” on page 219 for details about changing the order of a filter.
Attributes	Link to view attributes defined in the filter

- See Also**
- [Service Now Incident Filters Overview on page 207](#)
 - [Modifying an Incident Filter on page 214](#)
 - [Exporting Incident Filters on page 218](#)
 - [Reordering Incident Filters on page 219](#)
 - [Enabling Incident Filters on page 220](#)
 - [Disabling Incident Filters on page 221](#)
 - [Deleting Incident Filters on page 216](#)

Creating Incident Filters

This topic provides the details for creating basic and advanced filters and importing incident filters into Junos Space Service Now.

- [Creating a Basic Incident Filter on page 210](#)
- [Creating an Advanced Incident Filter on page 212](#)
- [Importing Incident Filters to Service Now on page 213](#)

Creating a Basic Incident Filter

A basic incident filter uses the *and* and *or* predefined computational logic on the JMB attributes to filter a JMB. You can use the following JMB attributes to define a basic incident filter:

- Event Synopsis
- Description
- Device IP Address
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name

For example, you can have a basic incident filter to filter JMBs that have the event type set to *Daemon Crash* and the event synopsis does not contain the term *mgd*.

To create a basic incident filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Create Basic Filter**.

The Create Basic Filter page appears as shown in [Figure 50 on page 211](#).

Figure 50: Create Basic Filter Page for Creating Basic Incident Filters

2. In the **Name** text box, enter a name for the filter.

An incident filter name can have a maximum of 255 alphanumeric characters. Special characters are not allowed.

3. In the **Action** list, select an action for the filter:

- Create Incident
- Do Not Create an Incident

4. For **Term Criteria**, select one of the following:

- All—An incident is created or not created for a JMB (depending on the selected action) only when the JMB matches all the terms defined in the filter.
- Any—An incident is created or not created for a JMB (depending on the selected action) when the JMB matches any of the terms defined in the filter.

5. Select a JMB attribute from the list stating **Select attribute type**.

6. Select a condition from the list stating **Select attribute condition**.

An attribute condition defines the conditions such as words that can be present or not present in an event synopsis, the date before or after which the event occurs, or specific platforms. The conditions listed in this drop-down list differ for each attribute.

For example: The Platform attribute has conditions such as includes, does not include, and starts with.

7. Enter a value in the next text box for the attribute selected in step 5 and condition selected in step 6.

For example, for the platform attribute, you can enter a value of SRX3400, EX3200, or MX960 so that the filter term is "Platform includes SRX3400" or "Platform does not include SRX3400".



NOTE: You can add only one value for an attribute and a condition in the text box.

8. Click **Add Term** to add new filter terms and repeat steps 5 to 7.



TIP: Click **Delete** to delete a filter term.

9. Click **Submit** to create the basic incident filter or click **Cancel** to cancel creating the filter.

After you click Submit, Service now creates the filter and lists the newly created filter on the Incident Filters page.

Creating an Advanced Incident Filter

An advanced filter uses Perl scripts to define the filter terms and provides you the flexibility to define your own filtering logic. You can use the following JMB attributes to define a filter term in an advanced filter:

- Event Synopsis
- Description
- Junos OS Version
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name
- Device ID

"Perl script" on page 457 is an example of an advanced incident filter:



NOTE: JMB attributes used in an advanced filter are assigned ARG values. For example, Device host name is assigned \$ARGV[1]. Do not change the ARG value of a JMB attribute.

To create an advanced incident filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Create Advanced Filter**.

The Create Advanced Filter page appears as shown in [Figure 51 on page 213](#).

Figure 51: Create Advanced Filter Page for Creating Advanced Incident Filters

2. In the **Name** text box, enter a name for the filter.
An incident filter name can have a maximum of 255 alphanumeric characters. Special characters are not allowed.
3. In the **Action** drop-down menu, select an action for the filter:
 - Create Incident
 - Do Not Create an Incident
4. (Optional) If the **Note** section is not expanded, click the down arrow icon next to Note to expand the Note section. The Note section provides a sample Perl script for filtering JMBs.
5. Click **Browse** and navigate to the Perl script on your local system.
The Perl script should have the **.pl** extension.
6. Click **Upload** to upload the Perl script.
When the upload is complete, Service Now displays a message indicating that the file is uploaded successfully.

Importing Incident Filters to Service Now

Service Now allows you to import both advanced and basic incident filters. You can use the import option to restore incident filters from an XML file in Service Now after an upgrade.

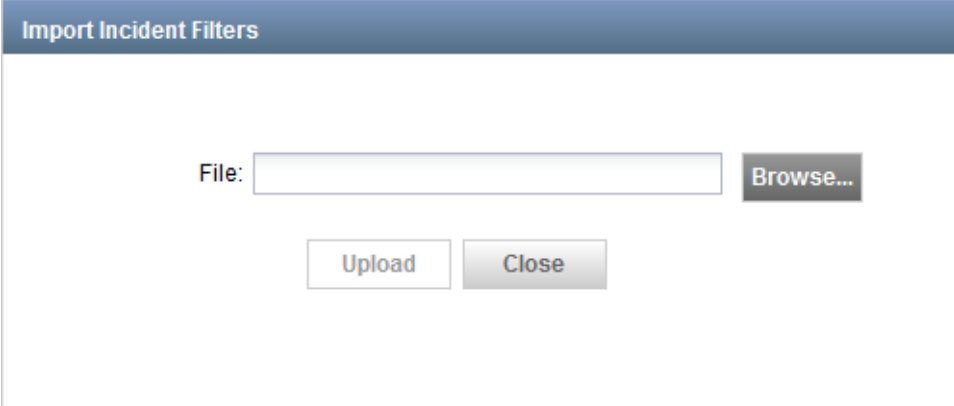
Imported filters are assigned the next available order, that is, when there are two filters in Service Now with orders 1 and 2, the imported filters are assigned order from 3 onwards.

To import incident filters to Service Now:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Import Incident Filters**.

The Import Incident Filters dialog box appears as shown in [Figure 52 on page 214](#).

Figure 52: Import Incident Filters Dialog Box



2. Click **Browse** and navigate to locate the file to be imported on your local system.

The file to be imported should be in the ***.xml** format.

3. Select the file and click **Upload** to upload the incident filters.

Service Now displays a message indicating that the file is uploaded successfully. You can view the uploaded filters on the Incident Filters page.

- See Also**
- [Service Now Incident Filters Overview on page 207](#)
 - [Modifying an Incident Filter on page 214](#)
 - [Exporting Incident Filters on page 218](#)
 - [Reordering Incident Filters on page 219](#)
 - [Enabling Incident Filters on page 220](#)
 - [Deleting Incident Filters on page 216](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)

Modifying an Incident Filter

Junos Space Service Now provides Modify option on the Actions list on the Incident Filters page to modify an Incident filter. You can modify the following parameters of the incident filter:

- Name of the filter
- Filter action
- Filter terms

To modify an incident filter:

1. From the Service Now navigation tree, click **Administration > Incident Filters**.

The Incident Filters page appears.

2. Select the filter that you want to modify and select **Modify** from the Actions list or right-click menu.

The Modify Basic Filter page or the Modify Advanced Filter page appears depending on the filter you chose to modify.

Figure 53 on page 215 shows the Modify Basic Filter page for modifying basic incident filters.

Figure 53: Modify Basic Filter Page for Modifying a Basic Incident Filter

Modify Basic Filter

Name:

Action:

Term Criteria: ☒ All (AND Term criteria) ☐ Any (OR Term criteria)

Event Occured Date	after	05/17/2017	4:23 AM	Delete
Event Synopsis	is not	Checknts_Starts_With_CHAS		Delete

Add Term

Submit Cancel

3. Modify the filter parameters—name, action, and filter terms.

For an advanced filter, you can upload a new Perl script defining new terms to modify one or more filter terms..

4. Click **Submit** to submit the changes.

Service Now displays a message indicating successful modification of the incident filter.

- See Also**
- [Service Now Incident Filters Overview on page 207](#)
 - [Viewing Incident Filters Configured on Junos Space Service Now on page 209](#)
 - [Creating Incident Filters on page 210](#)
 - [Exporting Incident Filters on page 218](#)
 - [Reordering Incident Filters on page 219](#)
 - [Enabling Incident Filters on page 220](#)
 - [Disabling Incident Filters on page 221](#)
 - [Modifying an Auto Submit Filter on page 230](#)

Deleting Incident Filters

Service Now provides the Delete option on the Action list to delete an Incident filter.

When you delete an incident filter, Service Now does not change the orders of the remaining filters. However, you can reorder the filters to change their order. For example, when there are four filters with orders 1, 2, 3, and 4 and if the filter with order 3 is removed, the remaining filters have the orders 1, 2, and 4.

To delete an incident filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

The Incident Filters page appears.

2. Select one or more filters that you want to delete and select **Delete** from the Actions list or the right-click menu.

The Delete Incident Filters dialog box appears as shown in [Figure 54 on page 217](#).

Figure 54: Delete Incident Filters Dialog Box

3. Click **Delete** to delete the selected filters or click **Cancel** to cancel deleting the filters.

Service Now displays a message indicating that the selected filters are deleted and the removes them from the Incident Filters page.

- See Also**
- [Service Now Incident Filters Overview on page 207](#)
 - [Viewing Incident Filters Configured on Junos Space Service Now on page 209](#)
 - [Creating Incident Filters on page 210](#)
 - [Modifying an Incident Filter on page 214](#)
 - [Exporting Incident Filters on page 218](#)
 - [Reordering Incident Filters on page 219](#)
 - [Disabling Incident Filters on page 221](#)
 - [Deleting Auto Submit Filters on page 239](#)

Exporting Incident Filters

Service Now provides the Export option on the Actions list of the Incident Filters page to export all or selected incident filters. The filters are exported in the *.xml format.

To export one or more incident filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.
The Incident Filters page appears.
2. Select one or more filters that you want to export and select **Export** from the Actions list or the right-click menu.

The Export Incident Filters dialog box appears as shown in [Figure 55 on page 218](#).

Figure 55: Export Incident Filters Dialog Box



3. Do one of the following to export one or more incident filters:
 - To export selected filters, click **Export Selected**.
 - To export all filters, click **Export All**.

The Export Job Status dialog box appears. A **Download** link appears in 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.
The browser displays a dialog box to view or save the exported file.
5. Click the option to view the XML file or click the option to save the XML file on your local system.

- See Also**
- [Exporting Auto Submit Filters on page 233](#)
 - [Service Now Incident Filters Overview on page 207](#)
 - [Reordering Incident Filters on page 219](#)
 - [Enabling Incident Filters on page 220](#)

Reordering Incident Filters

Order of a filter indicates the order in which a filter is applied to JMBs. A filter with order 1 is applied to a JMB before applying a filter with order 2. By default, a new filter is assigned the least order (highest number). Service Now provides the ReOrder Incident Filters option on the Actions list of the Incident filters page to re-order the incident filters.

To reorder incident filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

The Incident Filters page appears.

2. Select the filter and select **ReOrder Incident Filters** from the Actions list or right-click menu.

The Re-order Filters page appears as shown in [Figure 56 on page 219](#).

Figure 56: Re-order Filters page for Reordering Incident Filters

Filter Name	Filter Type	Filter Action	created By	Order	Status
<input type="checkbox"/> test_basic_filter_After	Basic	Do not create Incident	super	2	Enabled
<input type="checkbox"/> Test	Advanced	Do not create Incident	super	3	Enabled

3. Select the filter that you want to reorder and select the up or down arrow present above the list of filters to move the filter in the upward or downward direction.

As the filter is moved, its order also changes. The order of the filter increases when you move the filter in the upward direction and decreases when you move the filter in the downward direction.

4. Click **Save**.

Service Now saves the new order of the filters and displays the new order on the Incident Filters page.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Service Now Incident Filters Overview on page 207](#)

Enabling Incident Filters

After you create an incident filter, you must enable the incident filter before it is applied to a JMB. Service Now provides the Enable option on the Actions list to enable incident filters. The Status column on the Incidents page displays whether the incident filter is enabled or disabled.

To enable one or more incident filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

The Incident Filters page appears.

2. Select one or more filters that you want to enable and select **Enable** from the Actions list or right-click menu.

The Enable Incident Filters dialog box appears as shown in [Figure 57 on page 220](#).

Figure 57: Enable Incident Filters Dialog Box



3. Click **Enable** to enable the selected filters.

Service Now changes the status of the selected filters to Enabled on the Incident Filters page.

- See Also**
- [Enabling Auto Submit Filters on page 236](#)
 - [Disabling Incident Filters on page 221](#)
 - [Deleting Incident Filters on page 216](#)
 - [Service Now Incident Filters Overview on page 207](#)

Disabling Incident Filters

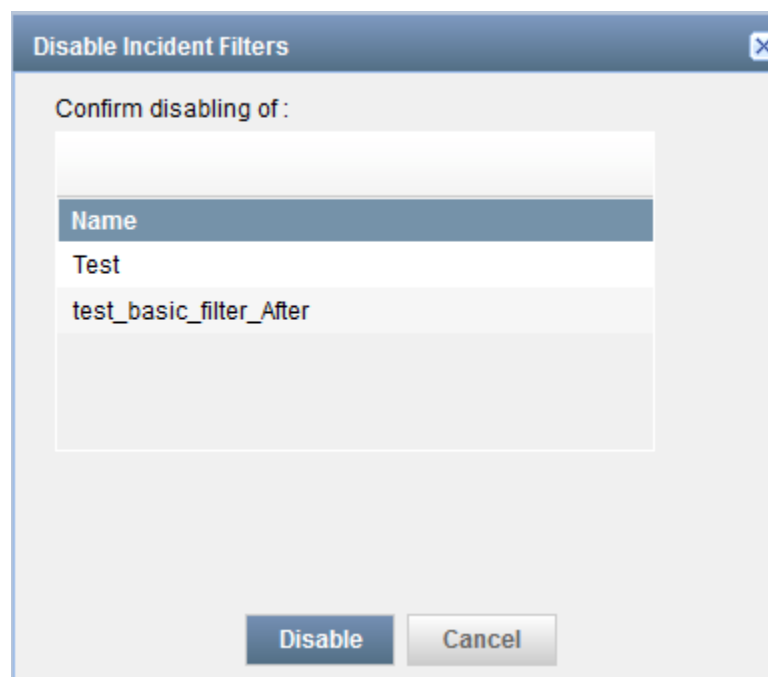
Service Now provides the Disable option on the Actions list to disable incident filters. A disabled filter cannot be used for filtering JMBs. Service Now displays whether an incident filter is enabled or disabled in the Status column of the Incident Filters page.

To disable one or more incident filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.
The Incident Filters page appears.
2. Select one or more filters that you want to disable and select **Disable** from the Actions list or the right-click menu.

The Disable Incidents Filters dialog box appears as shown in [Figure 58 on page 221](#).

Figure 58: Disable incident Filters Dialog Box



3. Click **Disable** to disable the selected filters.

Service Now changes the status of the filter to Disabled on the Incident Filters page.

- See Also**
- [Disabling Auto Submit Filters on page 237](#)
 - [Enabling Incident Filters on page 220](#)
 - [Creating Incident Filters on page 210](#)
 - [Service Now Incident Filters Overview on page 207](#)

Auto Submit Filters

- [Service Now Auto Submit Filters Overview on page 222](#)
- [Viewing Auto Submit Filters on page 225](#)
- [Creating Auto Submit Filters on page 226](#)
- [Modifying an Auto Submit Filter on page 230](#)
- [Exporting Auto Submit Filters on page 233](#)
- [Reordering Auto Submit Filters on page 234](#)
- [Enabling Auto Submit Filters on page 236](#)
- [Disabling Auto Submit Filters on page 237](#)
- [Assigning an Auto Submit Filter to a Domain on page 238](#)
- [Deleting Auto Submit Filters on page 239](#)

Service Now Auto Submit Filters Overview

Junos Space Service Now receives a Juniper Message Bundle (JMB) from a device, when an event occurs on the device, and creates an incident for the event. If auto submit policies are configured, Service Now automatically submits incidents to Juniper Support Systems (JSS) or Service Now partner for creating a case. Starting from Junos Space Service Now Release 17.1R1, you can assign auto submit filters to an auto submit policy to provide options for filtering incidents at a granular level before submitting them to JSS or a Service Now partner (in case of End Customer mode).

You can use the auto submit filters for the following purposes:

- Define incidents that should be submitted for creating cases
- Define incidents that should not be submitted for creating cases

Service Now displays all the configured auto submit policy filters on the Auto Submit Filters page (**Administration > Auto Submit Filters**) and provides options to define a basic filter, advanced filter, and import auto submit filters.

Basic filters filter incidents based on attributes such as event synopsis, platform, event type and so on by using the *and* and *or* predefined computational logic. Advanced filters use Perl script to define the filtering logic and thereby provide the flexibility to define your own filtering logic.

**NOTE:**

- Auto submit filters cannot be applied on incidents created for on-demand JMBs, BIOS JMBs, and Product Health Data JMBs.
- In a Service Now partner, auto submit filters cannot be applied to incidents received from a Service Now end customer.
- There is no limit on the number of auto submit filters that can be created. However, a large number of auto submit filters impacts the performance of Service Now when submitting incidents to JSS or Service Now partner.

Starting with Service Now Release 17.2R1, you can use in-built or custom Perl modules in advanced auto submit filters. For example, you can use custom Perl module for implementing a filtering logic and use that filtering logic across multiple advanced auto submit filters.

For using a Perl module, you can store the Perl module (*.pm) in any desired location in the Junos Space server and ensure that the files have read and executable permissions and the files are accessible by the advanced filters.

Starting with Service Now 17.2R1 release, auto submit filters are stored at the `/var/cache/jboss/sn/advanced_filter` location of the Junos Space server.



NOTE: The Perl module in-built in Service Now includes an API, `getExistingIncidents()`, for getting information about the latest 20 incidents. The API is included in the `FilterUtilV1.pm` file stored in `/var/cache/jboss/SN/AdvancedFilters`. For more information, see [“Sample Perl Script for Incident and Auto Submit Filters”](#) on page 457.

To view auto submit filters configured on Service Now, in the Service Now navigation tree, click **Administration > Auto Submit Filters**. The Auto Submit Filters page appears as shown in [Figure 59 on page 223](#). Double-clicking a filter opens the Auto Submit Filter Detail page that displays the details of the filter.

Figure 59: Auto Submit Filters Page

Administration > Auto Submit Filters								
Actions			0 Item Selected					
Name	Type	Action	Created By	Status	Created Time	Updated Time	Order	Associated Case
test_basic_filter_Platform_1	Basic	Associate to an existing Case	super	Enabled	May 22, 2017 2:14:36 PM IST	May 22, 2017 2:14:36 PM IST	1	2017-0517-0541
test_basic_filter_DESC_1	Basic	Do not Submit Case	super	Enabled	May 22, 2017 11:59:38 AM IST	May 22, 2017 11:59:38 AM IST	2	---

[Table 21 on page 223](#) lists the attributes of the auto submit filter displayed on the Auto Submit Filters and Auto Submit Filter Detail page.

Table 21: Fields on Auto Submit Filters Page

Column	Description
Name	Name of the auto submit filter.

Table 21: Fields on Auto Submit Filters Page (continued)

Column	Description
Type	Type of auto submit filter: Basic or Advanced.
Action	Action to be taken on an incident when the incident matches the conditions of the filter term: Submit case, Do not submit case, or Associate to an existing case.
Created By	User who created the filter.
Status	Status of the filter: Enabled or Disabled.
Created Time	Date and time when the filter is created.
Updated Time	Date and time when the filter was last updated.
Order	Order in which filters are applied to Incidents. By default, the filters are displayed in the ascending order. See “Reordering Auto Submit Filters” on page 234 for changing the order of a filter.
Associated Case ID	ID of the case to which an incident should be associated.
Associated Policy	Auto submit policies in which the auto submit filter is used.
Attributes	Link to view attributes defined in the filter.

Actions That You Can Perform From the Auto Submit Filters Task

You can perform the following actions related to auto submit filters:

- View Auto Submit filters; see [“Viewing Auto Submit Filters” on page 225](#) for details.
- Create Auto Submit filters; see [“Creating Auto Submit Filters” on page 226](#) for details.
- Modify Auto Submit filters; see [“Modifying an Auto Submit Filter” on page 230](#) for details.
- Delete Auto Submit filters; see [“Deleting Auto Submit Filters” on page 239](#) for details.
- Export Auto Submit filters; see [“Exporting Auto Submit Filters” on page 233](#) for details.
- Reorder Auto Submit filters; see [“Reordering Auto Submit Filters” on page 234](#) for details.
- Enable Auto Submit filters; see [“Enabling Auto Submit Filters” on page 236](#) for details.
- Disable Auto Submit filters; see [“Disabling Auto Submit Filters” on page 237](#) for details.


- See Also**
- [Service Now Incident Filters Overview on page 207](#)
 - [Service Now Suppressed Events Overview on page 380](#)
 - [Configuring Advanced Filter Settings on page 205](#)
 - [Service Now Auto Submit Policy Overview on page 241](#)

Viewing Auto Submit Filters

You can view auto submit filters that are configured on Service Now on the Auto Submit Filters page.

To view auto submit filters configured on Service Now, in the Service Now navigation tree, click **Administration > Auto Submit Filters**. The Auto Submit Filters page appears as shown in [Figure 60 on page 225](#).

Figure 60: Auto Submit Filters Page



Name	Type	Action	Created By	Status	Created Time	Updated Time	Order	Associated Case ID
test_basic_filter_Platform_1	Basic	Associate to an existing Case	super	Enabled	May 22, 2017 2:14:36 PM IST	May 22, 2017 2:14:36 PM IST	1	2017-0517-0541
test_basic_filter_DESC_1	Basic	Do not Submit Case	super	Enabled	May 22, 2017 11:59:38 AM IST	May 22, 2017 11:59:38 AM IST	2	---

[Table 22 on page 225](#) lists the information about auto submit filters displayed on the Auto Submit Filters page.

Table 22: Fields on Auto Submit Filters Page

Column	Description
Name	Name of the auto submit filter
Type	Type of auto submit filter: Basic or Advanced
Action	Action to be taken on an incident when the incident matches the conditions of the filter term: Submit case, Do not submit case, or Associate to an existing case
Created By	User who created the filter
Status	Status of the filter: Enabled or Disabled
Created Time	Date and time when the filter is created
Updated Time	Date and time when the filter was last updated
Order	Order in which filters are applied to Incidents. By default, the filters are displayed in the ascending order See "Reordering Auto Submit Filters" on page 234 for changing the order of a filter.
Associated Case ID	ID of the case to which an incident should be associated
Associated Policy	Auto submit policies in which the auto submit filter is used
Attributes	Link to view attributes defined in the filter

- See Also**
- [Viewing Incident Filters Configured on Junos Space Service Now on page 209](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)

- [Service Now Auto Submit Policy Overview on page 241](#)

Creating Auto Submit Filters

This topic provides the details for creating basic and advanced filters and importing auto submit filters to Junos Space Service Now.

- [Creating a Basic Auto Submit Filter on page 226](#)
- [Creating an Advanced Auto Submit Filter on page 228](#)
- [Importing Auto Submit Filters to Service Now on page 230](#)

Creating a Basic Auto Submit Filter

A basic auto submit filter uses the the *and* and *or* predefined computational logic on the incident attributes to filter an incident for submitting to JSS or Service Now partner (in case of End Customer mode). You can use the following incident attributes to define a basic auto submit filter:

- Event Synopsis
- Description
- Device IP Address
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name
- Device ID

For example, you can have a basic auto submit filter to filter incidents that have event type set to *Daemon Crash* and the event synopsis does not contain the term *mgd*.

To create a basic auto submit filter:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters > Create Auto Submit Filter**.

The Create Basic Filter page appears as shown in [Figure 61 on page 227](#).

Figure 61: Create Basic Filter for Creating a Basic Auto Submit Filter

2. In the **Name** text box, enter a name for the filter.
The name can have alphanumeric characters.
The name of an auto submit filter can have a maximum of 255 alphanumeric characters. Special characters are not allowed.
3. In the **Action** list, select an action for the filter:
 - Submit Case
 - Do Not Submit Case
 - Associate to an Existing Case.
4. For **Term Criteria**, select a term criteria as follows:
 - All—The action defined in step 3 is performed only when the incident matches all the terms defined in the filter.
 - Any—The action defined in step 3 is performed only when the incident matches any of the terms defined in the filter.
5. Select an incident attribute from the list stating **Select an attribute type**.
6. Select a condition from the list stating **Select attribute condition**.
An attribute condition defines the conditions such as words that can be present or not present for an attribute. The conditions listed in this list differ for each attribute.
For example, the Platform attribute has conditions such as includes, does not include, and starts with.
7. Enter a value in the next text box for the attribute selected in step 5 and condition selected in 6.

For example, for the platform attribute, you can enter a value of SRX3400, EX3200, or MX960 so that the filter term is "Platform includes SRX3400" or "Platform does not include EX3400".



NOTE: You can add only one value for an attribute and a condition in the text box.

8. Click **Add Term** to add new filter terms and repeat steps 5 to 7.



TIP: Click **Delete** to delete a filter term.

9. Click **Submit** to create the basic auto submit filter.

After you click submit, the filter is created and listed on the Auto Submit Filters page.

Creating an Advanced Auto Submit Filter

An advanced filter uses Perl scripts to define the filter terms and provides you the flexibility to define your own filtering logic. You can use the following incident attributes to define a filter term in an advanced filter:

- Event Synopsis
- Description
- Junos OS Version
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name

"Perl script" on page 457 is an example of an advanced auto submit filter:



NOTE: JMB attributes used in an advanced filter are assigned ARG values. For example, Device host name is assigned \$ARGV[1]. Do not change the ARG value of a JMB attribute.

To create an advanced auto submit filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Create Advanced Filter**.

The Create Advanced Filter page appears as shown in [Figure 62 on page 229](#).

Figure 62: Create Advanced Filter Page for Creating an Advanced Filter

2. In the **Name** text box, enter a name for the filter.
The name of an auto submit filter can have a maximum of 255 alphanumeric characters. Special characters are not allowed.
3. In the **Action** list, select an action for the filter:
 - Submit Case
 - Do Not Submit Case
 - Associate to an Existing Case.
4. (Optional) If the **Note** section is not expanded, click the down arrow icon next to Note to expand the Note section.
The Note section provides a sample Perl script for filtering JMBs.
5. Click **Browse** and navigate to the Perl script stored on your local system.
The Perl script should have the extension **.pl**.
6. Click **Upload** to upload the Perl script.
When the upload is complete, a message indicating that the file is uploaded successfully is displayed.

Importing Auto Submit Filters to Service Now

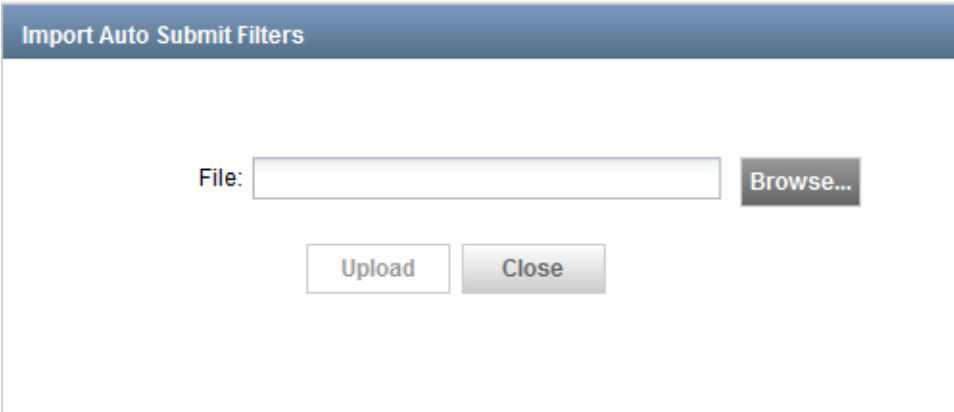
Service Now allows you to import both advanced and basic auto submit filters. You can use the import option to restore filters from an XML file in Service Now after an upgrade.

To import auto submit filters to Service Now:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Import Incident Filters**.

The Import Auto Submit Filters dialog box appears as shown in [Figure 63 on page 230](#).

Figure 63: Import Auto Submit Dialog Box

The image shows a dialog box titled "Import Auto Submit Filters". It contains a "File:" label followed by a text input field and a "Browse..." button. Below these are two buttons: "Upload" and "Close".

Import Auto Submit Filters

File: [Browse...](#)

[Upload](#) [Close](#)

2. Click **Browse** and navigate to locate the file to be imported on your local system.

The file to be imported should be in the *.xml format.

3. Select the file and click **Upload** to upload filters.

A message indicating that the file is uploaded successfully is displayed.

- See Also**
- [Creating Incident Filters on page 210](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)

Modifying an Auto Submit Filter

Junos Space Service Now provides the Modify option on the Actions list of the Auto Submit Filters page to modify an auto submit filter. You can modify the following parameters of the auto submit filter:

- Name of the filter
- Filter action
- Filter terms

To modify an auto submit filter:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

The Auto Submit Filters page appears.

2. Select the filter that you want to modify and select **Modify** from the Actions list or right-click menu.

The Modify Basic Filter or Modify Advanced Filter page appears depending on the filter you chose to modify. The Modify Advanced Filter page is shown in

[Figure 64 on page 231](#).

Figure 64: Modify Advanced Filter Page for Modifying an Advanced Auto Submit Filter

Modify Advanced Filter

Name:

Action:

Associate Case Id:

Note

Please upload a perl file for filtering incidents while submitting through auto submit policy.

Perl file should return either 0 (if JMB is matched with custom criteria) or -1 (if JMB is not matched with custom criteria).

Sample perl file [i](#)

Perl file:

3. Modify the filter parameters:

- Name
- aAction

- Associate Case Id if Action is set to Associate to an Existing Case
- Filter Terms

For an advanced filter, you can upload a new Perl script defining new terms to modify the filter term parameters.

4. Click **Submit** to submit the changes or click **Cancel** to cancel the changes.

A message indicating that the auto submit filter is successfully modified is displayed.

- See Also**
- [Modifying an Incident Filter on page 214](#)
 - [Exporting Auto Submit Filters on page 233](#)
 - [Reordering Auto Submit Filters on page 234](#)
 - [Deleting Auto Submit Filters on page 239](#)

Exporting Auto Submit Filters

Junos Space Service Now provides the Export option on the Actions list of the Auto Submit Filters page to export all the configured or selected auto submit filters. The filters are exported in the *.xml format.

```
<Filters>
  <snVersion>18.1R1</snVersion>
  <Filter>
    <FilterData>
      <created>1514896801840</created>
      <createdBy>super</createdBy>
      <domainId>2</domainId>
      <filterAction>2</filterAction>
      <filterName>Test</filterName>
      <filterSubAction>4</filterSubAction>
      <filterType>1</filterType>
      <lastUpdated>1514896801840</lastUpdated>
      <priority>1</priority>
      <status>1</status>
    </FilterData>
    <FilterAttributes>
      <FilterAttribute>
        <domainId>2</domainId>
        <filterAttributeCondition>starts with</filterAttributeCondition>

        <filterAttributeName>Entity</filterAttributeName>
        <filterAttributeValue>r</filterAttributeValue>
        <filterCondition>1</filterCondition>
        <filterId>53475</filterId>
        <priority>0</priority>
      </FilterAttribute>
    </FilterAttributes>
    <FilterFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:nil="true"/>
  </Filter>
</Filters>
```

To export one or more auto submit filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

The Auto Submit Filters page appears.

2. Select one or more filters that you want to export and select **Export** from the Actions or the right-click menu.

The Export Auto Submit Filters dialog box appears as shown in [Figure 65 on page 234](#).

Figure 65: Export Auto Submit Filters Dialog Box

3. Do one of the following:

- To export the selected filters, click **Export Selected**.
- To export all filters, click **Export All**.

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.

The browser displays the dialog box to view or save the exported file.

5. View or save the XML file on your local system.

Reordering Auto Submit Filters

Order of a filter indicates the order in which a filter is applied to incidents. A filter with order 1 is applied to an incident before applying a filter with order 2. By default, a new filter is assigned the least order (highest order number). Service Now provides the ReOrder Auto Submit Filters option on the Actions list of the Auto Submit Filters page to reorder the auto submit filters.

To reorder an auto submit filter:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.



The Auto Submit Filters page appears.

2. Click **Actions > ReOrder Auto Submit Filters**.

The Re-order Filters dialog box appears as shown in [Figure 66 on page 235](#).

Figure 66: Re-order Filters Dialog Box for Reordering Auto Submit Filters

Re-order Filters

<input type="checkbox"/>	Filter Name	Filter Type	Filter Action	created By	Order	Status	
<input type="checkbox"/>	test_basic_filter_check	Basic	Do not create Incident	super	1	Disabled	^
<input type="checkbox"/>	asas	Advanced	Do not create Incident	super	2	Disabled	
<input type="checkbox"/>	test_basic_filter	Basic	Do not create Incident	super	3	Disabled	
<input type="checkbox"/>	test_basic_filter_Event	Basic	Do not create Incident	super	4	Disabled	
<input type="checkbox"/>	test_basic_filter_SYNO	Basic	Do not create Incident	super	5	Disabled	
<input type="checkbox"/>	test_basic_filter_Entity	Basic	Do not create Incident	super	6	Disabled	
<input type="checkbox"/>	test_basic_filter_Description	Basic	Do not create Incident	super	7	Disabled	
<input type="checkbox"/>	test_basic_filter_DeviceName	Basic	Do not create Incident	super	8	Disabled	
<input type="checkbox"/>	as	Basic	Do not create Incident	super	9	Disabled	
<input type="checkbox"/>	test_basic_filter_DeviceIP	Basic	Do not create Incident	super	10	Disabled	
<input type="checkbox"/>	test_basic_filter_TIME	Basic	Do not create Incident	super	11	Disabled	
<input type="checkbox"/>	test_basic_filter	Basic	Do not create Incident	super	12	Disabled	v

Save

Cancel

3. Select the filter that you want to reorder and select the up or down arrow present above the list of filters to move the filter in the upward or downward direction.

As the filter is moved, its order also changes. The order of the filter increases when the filter is moved in the upward direction and decreases when the filter is moved in the downward direction.

4. Click **Save**.

The new order of the filters is saved and displayed on the Auto Submit Filters page.

- See Also**
- [Reordering Incident Filters on page 219](#)
 - [Modifying an Auto Submit Policy on page 248](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)

Enabling Auto Submit Filters

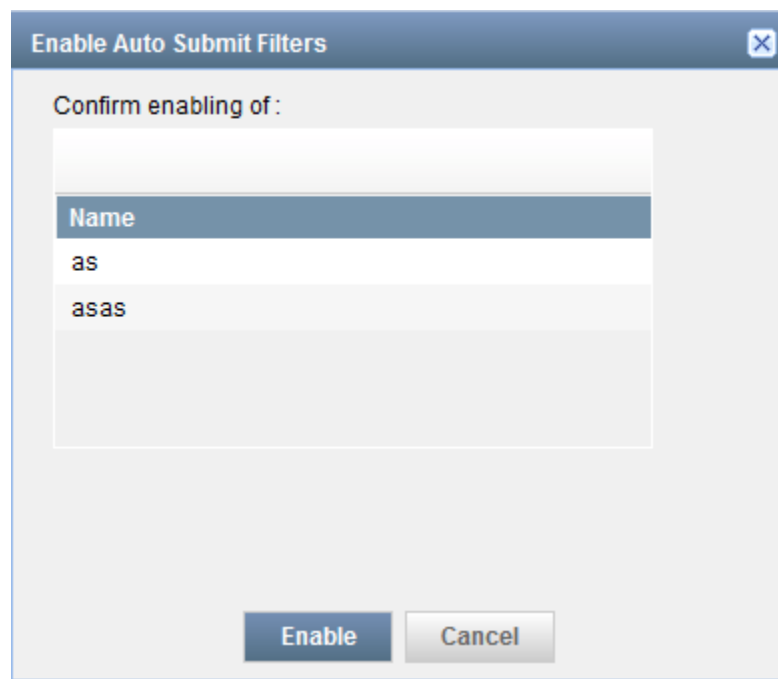
After you create an auto submit filter, you must enable the filter before it is applied to an incident. Service Now provides the Enable Auto Submit Filters option on the Actions list of the Auto Submit Filters page to enable auto submit filters. The Status column on the Auto Submit Filters page displays whether the auto submit filter is enabled or disabled.

To enable one or more auto submit filters:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

The Auto Submit Filters dialog box appears as shown in [Figure 67 on page 236](#).

Figure 67: Enable Auto Submit Filters Dialog Box



2. Select one or more filters that you want to enable and select **Enable Auto Submit Filters** from the Actions or the right-click menu.

The Enable Auto Submit Filters dialog box appears.

3. Click **Enable** to enable the selected filters.

The status of the selected filter changes to Enabled on the Auto Submit Filters page.

- See Also**
- [Enabling Incident Filters on page 220](#)
 - [Reordering Auto Submit Filters on page 234](#)
 - [Disabling Auto Submit Filters on page 237](#)

- [Service Now Auto Submit Policy Overview on page 241](#)
- [Service Now Auto Submit Filters Overview on page 222](#)

Disabling Auto Submit Filters

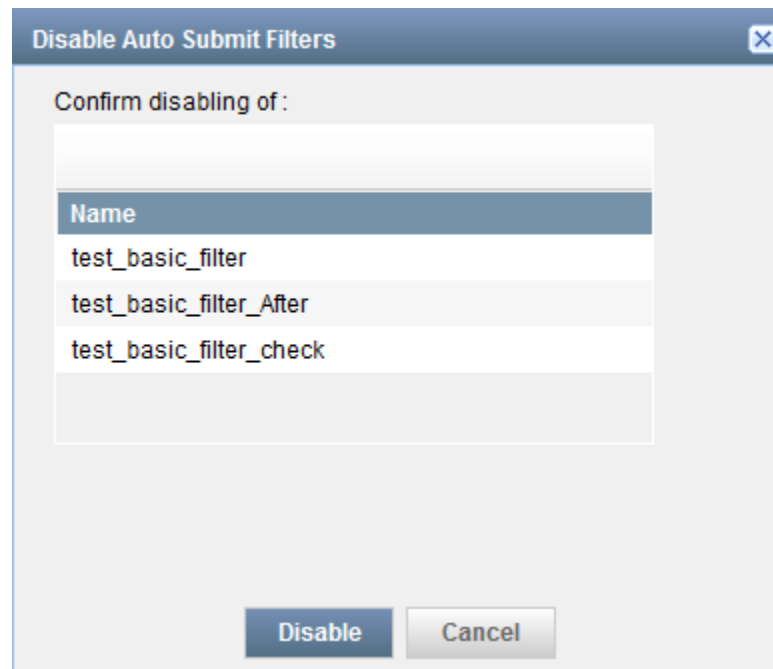
Junos Space Service Now provides the Disable Auto Submit Filters option on the Actions list of the Auto Submit Filters page to disable auto submit filters. A disabled filter cannot be used for filtering incidents for submitting to Juniper Support Systems (JSS) or Service Now partner.

To disable one or more auto submit filters:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

The Auto Submit Filters dialog box appears as shown in [Figure 68 on page 237](#).

Figure 68: Disable Auto Submit Filters Dialog Box



2. Select one or more filters that you want to enable and select **Disable** from the Actions list or the right-click menu.

The Disable Auto Submit Filters dialog box appears.

3. Click **Disable** to disable the selected filters.

The status of the selected filters is changed to disabled on the Auto Submit Filters page.

See Also • [Service Now Auto Submit Filters Overview on page 222](#)

Assigning an Auto Submit Filter to a Domain

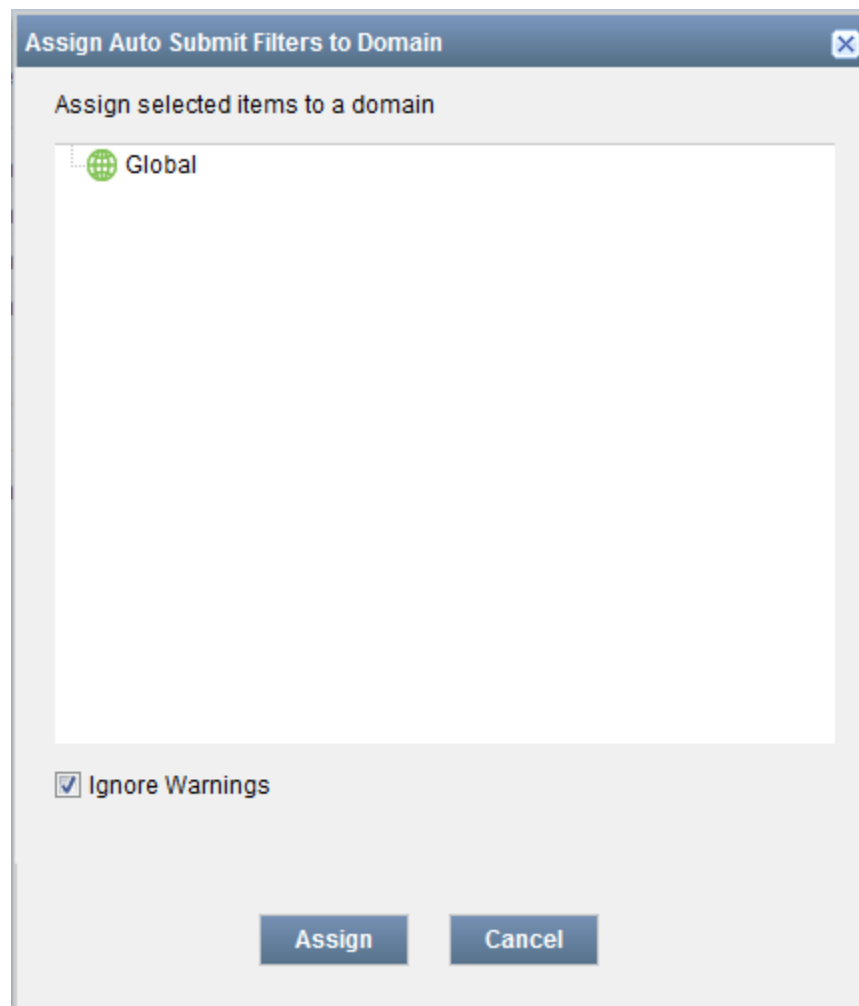
Service Now provides the Assign Incident Filters to Domain option to assign auto submit filters to a domain. By default, an auto submit filter is created in the domain to which the user is assigned.

To assign an auto submit filter to a domain:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

The Auto Submit Filters dialog box appears as shown in [Figure 69 on page 238](#).

Figure 69: Assign Auto Submit Filters to Domain Dialog Box



2. Select one or more filters that you want to assign to a domain and select **Assign Auto Submit Filters to Domain** from the Actions menu or the right-click menu.

The Assign Auto submit Filters to Domain dialog box appears.

3. In the Assign Auto Submit Filters to Domain dialog box, select the domain to which you want to assign the filter.
4. (Optional) Clear the **Ignore Warnings** check box to ignore any warnings that you may get while assigning the filter to a domain.
5. Click **Assign**.

A message is displayed indicating that the filters are assigned to the selected domain.

- See Also**
- [Assigning an Incident Filter to a Domain](#)
 - [Service Now Domain Overview on page 56](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)

Deleting Auto Submit Filters

Junos Space Service Now provides the Delete option on the Actions list of the Auto Submit Filters page to delete auto submit filters from the Auto Submit Filters page.

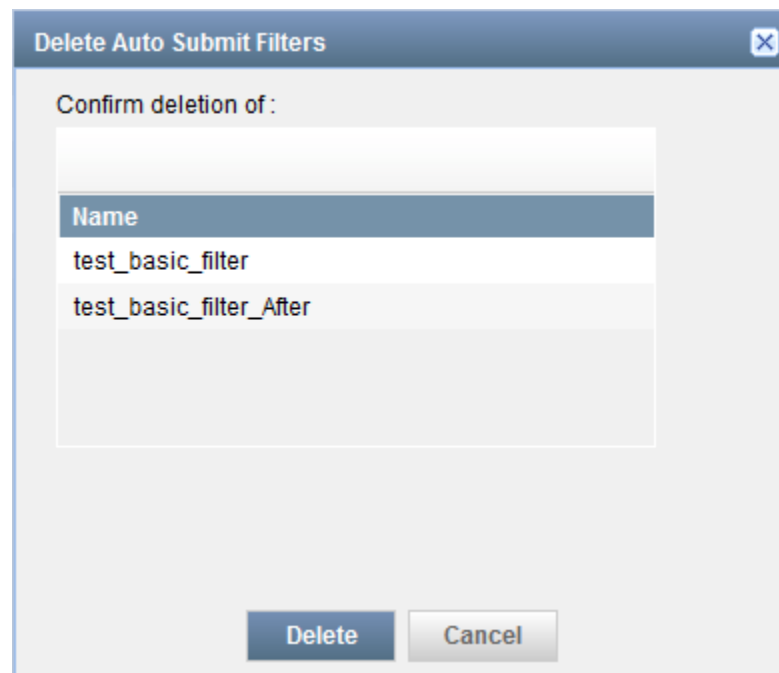


NOTE: You cannot delete an auto submit filter if it is associated with an auto submit policy. Therefore, before you attempt deleting an auto submit policy, ensure that filter that you are going to delete is not associated with any auto submit policy.

To delete an auto submit filter:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

The Auto Submit Filters dialog box appears as shown in [Figure 70 on page 240](#).

Figure 70: Delete Auto Submit Filters Dialog Box

2. Select one or more filters that you want to delete and select **Delete** from the Actions list or the right-click menu.

The Delete Auto Submit Filters dialog box appears.

3. Click **Delete** to delete the selected filters or click **Cancel** to cancel deleting the filters.

Service Now displays a message indicating that the auto submit filters are deleted successfully and removes the deleted filters from the Auto Submit Filters page.

See Also • [Service Now Auto Submit Filters Overview on page 222](#)

Auto Submit Policy

- [Service Now Auto Submit Policy Overview on page 241](#)
- [Creating an Auto Submit Policy on page 243](#)
- [Modifying an Auto Submit Policy on page 248](#)
- [Deleting Auto Submit Policies from Service Now on page 249](#)
- [Exporting an Incidents Report on page 250](#)
- [Changing the Status of Auto Submit Policies on page 251](#)
- [Changing the Dampening Status of an Auto Submit Policy on page 253](#)

Service Now Auto Submit Policy Overview

An auto submit policy allows Service Now to submit incidents to Juniper Support Systems or a Service Now partner (JSS) automatically. When Service Now submits an incident to JSS, JSS creates a technical support case and provides the case ID to Service Now. After a case is created in JSS, Service Now updates the status of the incident as Case Created along with the case number.

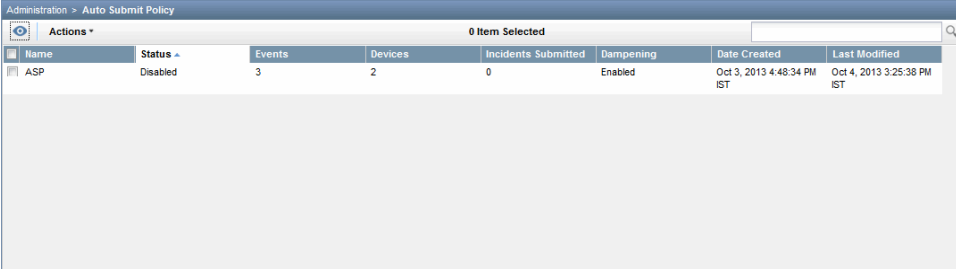
An auto submit policy lets you configure Service Now to prevent creating incidents when a JMB is received for the same event within a configured time interval. This is called dampening. Dampening policy is assigned to individual events if the Auto Submit Policy is activated. You can select a dampening period for which alerts are dampened for an event that recurs on the same device, device group, or organization.

Service Now displays the configured auto submit policies on the Auto Submit Policy page (**Administration > Auto Submit Policy**).

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 the incident for the last event is in the closed state, Service Now creates a new incident for the event; otherwise, Service Now does not create an incident. 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 71 on page 241](#).

Figure 71: 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

[Table 23 on page 241](#) lists the parameters of an auto submit policy.

Table 23: Auto Submit Policy Parameters

Parameter	Description
Name	Name of the auto submit policy.

Table 23: Auto Submit Policy Parameters (continued)

Parameter	Description
Status	<p>Status of the auto submit policy.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Enabled—The auto submit policy can be applied to devices for automatically submitting incidents for creating cases. • Disabled—The auto submit policy cannot be applied to devices for automatically submitting incidents for creating cases.
Events Count	Number of events included in the event profile.
Devices Count	Number of devices to which the auto submit policy is assigned.
Filters Count	Number of filters associated with the auto submit policy.
Incidents Submitted	Number of incidents submitted for creating case by using the auto submit policy.
Dampening	<p>Indicates whether incident creation should be dampened for the events included in the auto submit policy.</p> <p>NOTE: The dampening status for individual events override the dampening status of the auto submit policy.</p>
Created By	User who created the auto submit policy.
Created Date	Date and time the auto submit policy was created.
Last Modified	Date and time the auto submit policy was last modified.
Devices	Devices to which the auto submit policy is assigned.
Filters	Auto submit filters associated with the auto submit policy.
Events	Events included in the auto submit policy.

Associated Actions

You can perform the following actions related to auto submit policies:

- Change the status of one or more auto submit policies; see [“Changing the Status of Auto Submit Policies” on page 251](#) for details.
- Export details about the incidents created by using an auto submit policy; see [“Exporting an Incidents Report” on page 250](#) for details.
- Delete auto submit policies; see [“Deleting Auto Submit Policies from Service Now” on page 249](#) for details.
- Modify an auto submit policy; see [“Modifying an Auto Submit Policy” on page 248](#) for details.

- Change dampening status; see [“Changing the Dampening Status of an Auto Submit Policy” on page 253](#) for details.
- Assign an auto submit policy to another domain; see [“Assigning a Service Now Object to a Domain” on page 58](#) for details.

- See Also**
- [Creating and Editing a Notification Policy on page 386](#)
 - [Service Now Devices Overview on page 117](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)
 - [Service Now Suppressed Events Overview on page 380](#)

Creating an Auto Submit Policy

An auto submit policy enables Service Now to automatically submit incidents to JSS for creating a Tech Support Case. Although events with priority P1 can be included in an auto submit policy, Service Now does not submit incidents created for P1 events to JSS automatically. Therefore, incidents created for 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 72 on page 243](#).

Figure 72: Auto Submit Policy Creation Page

Administration > Auto Submit Policy > Create Auto Submit Policy

Choose devices to include in Auto Submit Policy

Policy Name:

Show:

[Show Selected Devices](#)

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle	Policy
JCare-Plus	Default for JCare-Plus	device1	33108	M10I	11.4R7.5	3.7R1.2	ASP
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	3.7R1.2	ASP
JCare-Plus	Default for JCare-Plus	device4	JN11B7992AEA	M120	11.4R7.5		
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		

Page 1 of 1

Displaying 1 - 7 of 7

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

The name can contain only alphanumeric (a-z, A-Z, 0-9), underscores (_), and hyphens (-). The maximum number of characters allowed is 255.

3. Select an option in the **Show** list as follows for assigning the auto submit policy to devices::

- To filter devices by their organization, in the **Show** list, select **By Organization** and select an *Organization* in the **Organization** list.

Service Now displays a list of devices belonging to the selected organization.

- To filter devices by device group, in the **Show** list, select **By Device Group** and select a *Device Group* from the **Device Group** list.

Service Now displays a list of devices belonging to the selected device group.

4. Select the devices for which you want to assign the auto submit policy.

5. (Optional) Click the **Show Selected Devices** link to view the list of devices selected for assigning the auto submit policy that you are creating.

The **Selected Devices** dialog box displays the list of devices that you selected. Verify the list and click **Close** to return to the previous page.

6. Click **Next**.

The **Choose events to include in Auto Submit Policy** page appears.

Figure 73: 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](#)

☐ Select All Events Across Pages [Duplicate Incident Dampening](#)

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

Displaying 1 - 50 of 442

Back Next Cancel

7. Select the events to be included in the auto submit policy by using one of the following options:




- Select the **Select All Events Across Pages** check box to include all the listed events to the auto submit policy.
- Manually select the events.

Events with priority P1 are not available for selection. Do not include events that are inactive for the selected devices.. You can easily identify these events by looking at the icons that are used to represent them (see [Table 24 on page 245](#)).



TIP: To find events, type the event name in the **Find event** search 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, when you type audi in the **Find event** search field, all events with names beginning with audi are listed.

Table 24: 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 you can include these events in the auto submit policy, Service Now does not automatically submit these incidents for creating cases to JSS or Service Now partner. You can open a case for these events only by contacting JSS directly over phone.

8. (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.
9. Click the **Duplicate Incident Dampening** link to set the dampening interval for the selected events. The Duplicate Incident Dampening dialog box appears.
10. Select a dampening interval from the **Dampen Incidents for** drop-down list for each event as follows:
 - **None:** Select None to create an incident for each occurrence of the events on the selected devices.
 - **Always:** Select Always if you do not want an incident to be created after the first occurrence of the event on the selected devices. Service Now does not create another incident for the event until the first incident is closed or deleted.
 - **Dampening intervals of 1hr, 2hr, 3hr, ...:** Service Now does not create incidents for the specified time duration after the first occurrence of the event. However, if the

first incident is closed or deleted within in the specified time duration, Service Now creates another incident for the same event.

11. Click **Next**.

The Choose filters to include in Auto Submit Policy page appears. This page lists the auto submit filters configured in Service Now and also provides the options to create basic and advanced auto submit filters, and reorder auto submit filters to change the order in which the filters are applied to incidents.

12. (Optional) Do one of the following tasks to assign auto submit filters to the auto submit policy:

- Select one or more auto submit filters to be associated with the auto submit policy.
- Click **Create Basic Filter** to create a basic auto submit filter and assign it to the auto submit policy.

For information about creating basic auto submit filters, see [“Creating a Basic Auto Submit Filter” on page 226](#).

- Click **Create Advanced Filter** to create an advanced auto submit filter and assign it to the auto submit policy.

For information about creating advanced auto submit filters, see [“Creating an Advanced Auto Submit Filter” on page 228](#).

- Click **Reorder Filters** to reorder the filters.

The Reorder Filters page appears. Change the order of the filter by selecting the filter and clicking the up or down arrow to change the order.



NOTE: The order of filters in an auto submit policy is relevant to only that policy. The same filters can be associated with another policy and have a completely different order.

13. Click the **Next** button to proceed with creating the auto submit policy.

The Submit Case Options page appears.

14. Click the **Enter Email Id** field to enter one or more e-mail IDs in the format user@example.com.

Service Now sends notifications to the configured e-mail IDs when the incident is created and when the status of the incident changes.

To add, or delete multiple e-mail IDs, use the **Add Email** and **Delete** buttons.

15. (Optional) Click **Modify** to modify the site ID or username of the 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 your organization in their respective fields. After your user credentials are validated, click **Get Sites** to select a site ID specific to the new user.

16. 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.

17. (Optional) Select the **Upload Associated Core Files for Incident** check box to upload core files generated for the incident.

18. (Optional) Select the **Upload All Core Files** check box if you want the auto submit policy to upload all core files available on the device to the configured SFTP server for selected events.

19. (Optional) Select the **Delete Core Files from devices after uploading** check box If you want to delete core files from the device after uploading it to the SFTP server.

You must select the **Delete Core Files from devices after uploading** in combination with the **Upload Associated Core Files for Incident** or **Upload All Core Files** check box.

When you select the **Delete Core Files from devices after uploading** check box in combination with the **Upload Associated Core Files for Incident** check box, the core files associated with the event are deleted from the device after the core file is uploaded to Service Now.

When you select the **Delete Core Files from devices after uploading** check box in combination with the **Upload All Core Files for Incident** check box, all core files present on the device are uploaded to Service Now and deleted from the device.

20. In the **Follow Up Method** list, select the method that you would like to use to follow up on the case associated with the incident—Email Full Text Update, Email Secure Web Link, or Phone Call.

21. In the **Priority** field, select the priority of the case.

The available options are Critical, High, Medium, and Low. The default priority is Low.

22. (Optional) In the **Minimum Incident Submission Delay Time (In Mins)** field, enter the number of minutes by which you want Service Now to delay submitting the incident for creating a case.

You can delay submitting an incident by 1 – 21600 minutes.

23. In the **Add Comments to Synopsis** and **Add Comments to Description** fields, enter a synopsis and description for the incident.

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 description is 255 and 1,028 respectively.

24. Click **OK**.

The auto submit policy is created and listed in the View Auto Submit Policy page. When the events selected in the auto submit policy occur on the devices associated with the auto submit policy, incidents are automatically submitted to Juniper Support Systems (JSS) and a Technical support case is created. For Service Now operating in End Customer mode, the incidents are submitted to Service Now partner.

Service Now submit incidents for creating a case by using an auto submit policy only when the policy is enabled. By default, auto submit policies are enabled. To disable auto submit policies, see [“Changing the Status of Auto Submit Policies” on page 251](#).

- See Also**
- [Assigning an Auto Submit Policy to a Device on page 148](#)
 - [Changing the Dampening Status of an Auto Submit Policy on page 253](#)
 - [Adding an SNMP Configuration to Service Now on page 194](#)
 - [Creating and Editing a Notification Policy on page 386](#)

Modifying an Auto Submit Policy

Junos Space Service Now provides the Modify option in the Actions list of the Auto Submit Policies page to modify auto submit policies. The Modify option lets you modify the following parameters of an auto submit policy:

- Devices assigned to the policy
- Dampening settings for the events included in the policy
- Auto submit filters associated with the policy
- Options such as priority, follow up method, dampening status, and delay time to submit the incidents

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 Modify Auto Submit Policy page appears.
3. In the Choose devices to Include in Auto Submit Policy section select or clear the check boxes provided on the first column of the devices table to include or exclude the devices from the auto submit policy.

4. (Optional) Click the **Show Selected Devices** link to view devices selected for including in the auto submit policy.

5. Click **Next**.

The Choose events to Include in Auto Submit Policy section appears.

6. (Optional) Modify the dampening settings of an incident by clicking the event on the dampening column and selecting a dampening value from the drop-down list.

None indicates that no incident is created and submitted for the event and *Always* indicates that an incident is always created and submitted for the event. The values such as *1 hr*, *2 hr*, *1 day*, or *3 days* indicate that the incident is submitted to JSS or Service Now partner after the 1 hr, 2 hr, 1 day, or 3 days.

7. Click **Next**.

The Choose filters to Include in Auto Submit Policy section appears.

8. (Optional) Select or clear the check boxes provided on the first column of the auto submit filters table to include or exclude the auto submit filters from the auto submit policy.

If you want to associate a new filter with the auto submit policy, click the **Create Basic Filter** or **Create Advanced Filter** links to create a basic or advanced auto submit filter respectively.

9. (Optional) Click the **ReOrder Filters** link to reorder the filters.

10. Click **Save**.

Your changes are saved and the auto submit policy is listed in the Auto Submit Policy page with your modifications.

- See Also**
- [Adding an SNMP Configuration to Service Now on page 194](#)
 - [Creating and Editing a Notification Policy on page 386](#)
 - [Assigning an Auto Submit Policy to a Device on page 148](#)

Deleting Auto Submit Policies from Service Now

Junos Space Service Now provides the Delete option in the Actions list of the Auto Submit Policies page to delete auto submit policies.

To delete auto submit policies:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**. The Auto Submit Policy page appears.

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

The Delete Policies dialog box appears.

3. Click **Delete** to confirm.

The selected auto submit policies are deleted and removed from the View Auto Submit Policy page.

- See Also**
- [Service Now Auto Submit Policy Overview on page 241](#)
 - [Creating an Auto Submit Policy on page 243](#)
 - [Modifying an Auto Submit Policy on page 248](#)
 - [Adding an SNMP Configuration to Service Now on page 194](#)
 - [Creating and Editing a Notification Policy on page 386](#)

Exporting an Incidents Report

Junos Space Service Now provides the Export Incident Report option in the Actions list of the Auto Submit Policies page to export details about incidents that Service Now submitted by using an auto submit policy.

Service Now exports the following information about an auto submit policy:

- Date and time the auto submit policy was used to submit an incident
- Event for which the auto submit policy was used to submit an incident
- Priority of the event
- Status of submitting the incident
- Host name, IP address, and the product family of the device on which the event occurred
- Version of AI-Scripts installed on the device

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 one or more auto submit policies for which you want to export incident report 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.

The browser displays the dialog box for you to open or save the Excel file.

4. Select one of the following options:
 - To open the Excel file, select **Open with** and click **Open**.
 - To save the Excel file on your local file system, select **Save File**, and navigate to the folder where you want to save the Excel file, and click **OK**.

You can view the incidents created by selected auto submit policies in the generated Excel file.

- See Also**
- [Modifying an Auto Submit Policy on page 248](#)
 - [Creating and Editing a Notification Policy on page 386](#)
 - [Adding an SNMP Configuration to Service Now on page 194](#)

Changing the Status of Auto Submit Policies

Service Now provides the Change Status option in the Actions list to enable or disable an auto submit policy. By default, an auto submit policy is enabled. Incidents can be submitted to Juniper Support Systems (JSS) or Service Now partner for creating a case 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 you want to change the status 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 74 on page 252](#).

Figure 74: Change Auto Submit Policy Status Page

Policy Name	Current Status
ASP	Disabled

☐

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**.
If you have not scheduled a time for changing the status, Service Now initiates the job to change auto submit policy status immediately after you click Change Status and displays the jobs dialog box; otherwise, Service Now initiates the job at the scheduled time..
5. (Optional) Click the *Job ID* link to view the status of the change status job.
6. After the job is complete, click **OK**.

The Quick View of the auto submit policy is displayed in the Auto Submit Policy page.

- See Also**
- [Modifying an Auto Submit Policy on page 248](#)
 - [Changing the Dampening Status of an Auto Submit Policy on page 253](#)
 - [Service Now Auto Submit Policy Overview on page 241](#)
 - [Creating an Auto Submit Policy on page 243](#)
 - [Creating and Editing a Notification Policy on page 386](#)
 - [Adding an SNMP Configuration to Service Now on page 194](#)

Changing the Dampening Status of an Auto Submit Policy

Junos Space Service Now provides the Change Dampening option on the Actions list of the Auto Submit Policies page 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).

Incidents are submitted for all events included in an auto submit policy only if the dampening status of the policy is enabled. However, you can configure Service Now to not submit an incident for an event included in the policy by setting the dampening status of the event to disabled. For information about modifying the dampening status of events in an event policy, see [“Modifying an Auto Submit Policy” on page 248](#)

To change the dampening status:

1. From the Service Now navigation tree, select **Administration > Auto Submit Policy**.

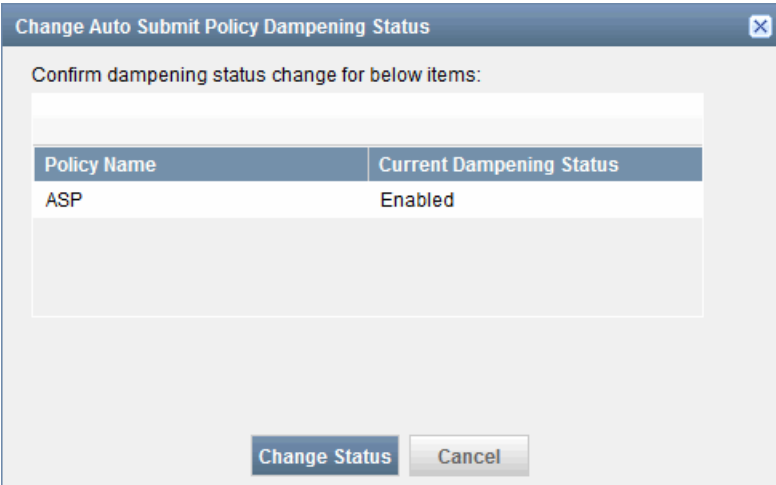
The Auto Submit Policy page appears

2. Select one or more auto submit policies for which you want to change the dampening status.

3. Click **Change dampening status** from either the **Actions** list or the right-click menu.

Service Now displays the Change Auto Submit Policy Dampening Status dialog box. See [Figure 75 on page 253](#).

Figure 75: 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.

See Also • [Service Now Auto Submit Policy Overview on page 241](#)

- [Creating and Editing a Notification Policy on page 386](#)
- [Adding an SNMP Configuration to Service Now on page 194](#)

Product Health Data Collection

- [Service Now Product Health Data Collection Overview on page 254](#)
- [Viewing Product Health Data Files Collected from a Device on page 256](#)
- [Product Health Data Collection Configuration Overview on page 259](#)
- [Configuring Product Health Data Collection on a Device on page 262](#)
- [Modifying a Product Health Data Collection Configuration on page 267](#)
- [Rescheduling a Product Health Data Collection Configuration on page 270](#)
- [Retrying Collecting Product Health Data from a Device on page 271](#)
- [Disabling Product Health Data Collection on a Device on page 273](#)
- [Enabling Product Health Data Collection on a Device on page 274](#)
- [Aborting a Product Health Data Collection Configuration on page 275](#)
- [Exporting Product Health Data Information to an Excel File on page 276](#)
- [Deleting Product Health Data Files Collected from a Device on page 281](#)
- [Deleting a Product Health Data Collection Configuration from Service Now on page 283](#)

Service Now Product Health Data Collection Overview

Starting from Service Now Release 15.1R1, Service Now collects product health data (PHD) from managed devices to assess the health of the devices.



NOTE:

- PHDC is not supported on Service Now operating in End Customer mode.
Starting in Service Now Release 16.1R1, a Service Now partner can collect PHD on end-customer devices.
- 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 is composed of 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 256](#).

Figure 76 on page 255 shows the Product Health Data Devices page that lists the devices from which Service Now collects PHD. You can view the status of PHD collected on a device on this page. Service Now lists a device on this page when at least one PHD file is collected from it.

Figure 76: Product Health Data Devices Page

Device	Serial Number	Product	View
sn-220-sn1	AQ5210AA0078	SRX220H	View
sn-650-sn2	AJ4410AA0037	SRX650	View

Table 25 on page 255 describes the fields on the Product Health Data Devices page.

Table 25: 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
View	Link to view the PHD files collected from the device For information about viewing the PHD files, see “Viewing Product Health Data Files Collected from a Device” on page 256 .

Service Now submits the PHD collected to Juniper Support Systems (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 262](#)

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 276](#).

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Service Now BIOS Validation Overview on page 160](#)

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. Service Now uploads these files to Juniper Support Systems (JSS) for assessment. You can view the list of PHD files collected for a device on the View all Product Health Data Files page as shown in [Figure 77 on page 256](#). You can also download, export, and delete the PHD files by using this page.

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

Figure 77: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_20150416_162001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_152002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

Table 26: 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: <code>hostname-sys_phdc_jmb_ais_health_yyyymmdd_hhmmss</code>, where</p> <ul style="list-style-type: none"> • <code>hostname</code> is the hostname of the device from which PHD is collected. • <code>yyymmdd</code> is the date when PHD was collected. • <code>hhmmss</code> 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 it is collected 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.
Upload Status	<p>Status of uploading PHD files to JSS:</p> <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 78 on page 258](#).

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

Figure 78: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
snv-220-sn1	AG5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snv-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 a 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.

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

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

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

- See Also**
- [Service Now Product Health Data Collection Overview on page 254](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)
 - [Exporting Product Health Data Information to an Excel File on page 276](#)
 - [Deleting Product Health Data Files Collected from a Device on page 281](#)
 - [Deleting a Product Health Data Collection Configuration from Service Now on page 283](#)

Product Health Data Collection Configuration Overview

Starting from Service Now Release 15.1R1, Service Now provides the Product Health Data Collection feature to collect product health data (PHD) from managed devices for assessing devices' health. PHD is collected from a device by executing predefined Junos OS commands. For information about the Junos OS commands used for collecting PHD, see [Commands Used for Collecting PHD from Managed Devices](#)

You can configure Product Health Data Collection (PHDC) on Service Now operating in Direct, or Partner Proxy modes. Starting in Service Now Release 16.1R1, Service Now can collect PHD when operating in End Customer mode as well. However, uploading the end-customer product health data to Service Now partner is not supported.



NOTE: A Service Now partner cannot configure PHDC on end-customer devices.

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

- Devices on which PHD should be collected
- Number of days for which PHD should be collected
- Whether PHD data should be submitted to Juniper Support Systems (JSS) or Service Now partner

- Whether PHD data should be deleted from Service Now once uploaded to JSS or Service Now partner
- 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 79 on page 260](#).

Figure 79: 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 27 on page 260](#) lists the fields on the Product Health Data Collection page.

Table 27: 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 being 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 the date and time when PHD collection started
End Date	Date and time to end PHD collection or PHD collection ended (if the PHDC status is completed)

Table 27: Fields on the Product Health Data Collection Page (continued)

Field Name	Description
Devices	<p>Number of devices included in the PHDC configuration</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 “Service Now Product Health Data Collection Overview” on page 254 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>

Benefits of Product Health Data Collection

The Product Health Data Collection (PHDC) feature helps to confirm whether managed devices are maintaining performance expectations based on best practices recommended by Juniper Networks. The PHDC feature identifies potential malfunctioning of hardware components, dormant problems, any abnormalities in the trend data for improvement and any other performance related issues. Engineers at Juniper Networks analyze the product health data and recommend actions to customers to identify potential risks and issues with their devices before impacting their network and proactively improve network performance.

Actions That You Can Perform From the Product Health Data Collection Task

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

- Modify a PHDC configuration; see [“Modifying a Product Health Data Collection Configuration”](#) on page 267 for details.
- Reschedule a PHDC configuration; see [“Rescheduling a Product Health Data Collection Configuration”](#) on page 270 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 271 for details.
- Enable PHD collection on devices; see [“Enabling Product Health Data Collection on a Device”](#) on page 274 for details.
- Disable PHD collection on devices; see [“Disabling Product Health Data Collection on a Device”](#) on page 273 for details.
- Abort PHD collection on devices; see [“Aborting a Product Health Data Collection Configuration”](#) on page 275 for details.
- Delete a PHDC configuration; see [“Deleting a Product Health Data Collection Configuration from Service Now”](#) on page 283 for details.
- Assign a PHDC configuration to another domain; see [“Assigning a Service Now Object to a Domain”](#) on page 58 for details.

- See Also**
- [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Service Now Product Health Data Collection Overview on page 254](#)

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 methods to configure PHDC on managed devices:

- [Configuring PHDC by Using the Product Health Data Collection Task on page 262](#)
- [Configuring PHDC by Using the Service Now Devices Task on page 264](#)

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 80 on page 262](#).

Figure 80: Configure 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	5.020150722_2005_barmstrong
<input type="checkbox"/> Test-Org	Device Group for Test-Org	sn-3600-sn2	AB3510AA0022	SRX3600	12.1X44-D40.2	5.020150722_2005_barmstrong
<input type="checkbox"/> Test-Org	Device Group for Test-Org	corruption	JN1207242AJA	PTX5000	14.2R3	5.020150722_2005_barmstrong
<input type="checkbox"/> Test-Org	Device Group for Test-Org	r14ms960wf	JN1218FCCAFA	MX960	14.1-20150717.0	5.020150722_2005_barmstrong

2. Enter a name for the PHDC configuration.

The name of a PHDC configuration must have 4 to 64 alphanumeric characters. You can use underscore (_) and hyphen (-) as special characters.

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 81 on page 263](#).

Figure 81: Configure Product Health Data Collection

5. On the Configure Product Health Data Collection page, configure options as follows:
 - **Collection Period (days):** Enter the number of days when 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 Systems (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 a device 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 from the selected devices.

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, Service Now starts collecting PHD immediately after you submit 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 which is in Scheduled or Running state, you cannot assign the device to any other PHDC configuration.



NOTE: PHDC consumes CPU cycles and disk resources of a device. Therefore, performance might be affected while PHD is being 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 list, 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 82 on page 265](#).

Figure 82: Configure Product Health Data Collection Dialog Box

Configure Product Health Data Collection

Product 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, add devices to an existing or new PHDC configuration as follows:
 - 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**.

An option to select a PHDC configuration for assigning the selected devices appear.
 - 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**.

Options to configure a new PHDC appear.

- 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 Product Health Data Collection, 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 when Service Now should collect 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 if you want Service Now to upload PHD files collected from devices to Juniper Support Systems (JSS) or Service Now partner.

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 if you want Service Now 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 save the PHDC configuration.

If Service Now configures PHDC successfully, you can view the configuration on the Product Health Data Collection page (**Administration > Product Health Data Collection**).

If a time is scheduled, Service Now initiates PHD collection at the scheduled time. If a time is not scheduled, Service Now starts collecting PHD immediately after PHDC is configured.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Modifying a Product Health Data Collection Configuration on page 267](#)
 - [Rescheduling a Product Health Data Collection Configuration on page 270](#)
 - [Retrying Collecting Product Health Data from a Device on page 271](#)
 - [Disabling Product Health Data Collection on a Device on page 273](#)
 - [Enabling Product Health Data Collection on a Device on page 274](#)
 - [Aborting a Product Health Data Collection Configuration on page 275](#)
 - [Exporting Product Health Data Information to an Excel File on page 276](#)

Modifying a Product Health Data Collection Configuration

The parameters of a PHDC configuration that you can modify 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 list, 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 83 on page 269.

Figure 83: Modify Product Health Data Collection 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	5.020150722_0138
PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx320-sys	F7760	M320	12.3R8.7	5.020150722_0138
PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-mx240-sys	JN121EB69AFC	MX240	12.3R8.7	5.020150722_0138
PHD-Test-ORG	Default for PHD-Test-ORG	mx-480-sn2	JN11742FFAFB	MX480	12.3R6.6	5.020150722_0138

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

Service now displays the Modify Product Health Data Collection page.

Figure 84: Modify Product Health Data Collection Parameters

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**.

Service Now displays a message indicating the PHDC configuration is successfully modified..

- See Also**
- [Aborting a Product Health Data Collection Configuration on page 275](#)
 - [Disabling Product Health Data Collection on a Device on page 273](#)
 - [Retrying Collecting Product Health Data from a Device on page 271](#)
 - [Rescheduling a Product Health Data Collection Configuration on page 270](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)

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 259](#) for details on the status of PHDC configuration.

When you reschedule a PHDC configuration, the *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 list, 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.

When you click Submit, Service Now displays a message indicating that PHDC configuration is successfully rescheduled. If a date and time is not scheduled for PHD collection, Service Now starts collecting PHD immediately after you submit the configuration and changes the status of the PHDC configuration to Starting and then Running.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Aborting a Product Health Data Collection Configuration on page 275](#)
 - [Disabling Product Health Data Collection on a Device on page 273](#)
 - [Retrying Collecting Product Health Data from a Device on page 271](#)
 - [Modifying a Product Health Data Collection Configuration on page 267](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)

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 [“Service Now Product Health Data Collection Overview” on page 254](#) for details about the statuses of PHD collection on a device and [“Product Health Data Collection Configuration Overview” on page 259](#) 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 list, 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 85 on page 272](#). The page lists the devices in the configuration on which an earlier attempt to collect PHD failed.

Figure 85: Retry on Failed 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-m320-sys	F7760	M320	12.3R8.7	
<input type="checkbox"/> PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m240-sys	JN121EB69AFC	M240	12.3R8.7	
<input type="checkbox"/> 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.

When you click Submit, Service Now displays a message indicating that the 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.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Aborting a Product Health Data Collection Configuration on page 275](#)
 - [Disabling Product Health Data Collection on a Device on page 273](#)
 - [Rescheduling a Product Health Data Collection Configuration on page 270](#)
 - [Modifying a Product Health Data Collection Configuration on page 267](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)

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. The Disable 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:

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 in which you want to disable PHDC on one or more devices.

3. From the Actions list, 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 86 on page 273](#).

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

Figure 86: 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	K1915	M10i	11.4R7.5	
<input type="checkbox"/> PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m320-sys	F7760	M320	12.3R8.7	
<input type="checkbox"/> PHD-Test-ORG	Default for PHD-Test-ORG	sn-space-m240-sys	JN121EB69AFC	MX240	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, select 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.

On clicking Submit, Service Now displays a message indicating that the PHD collection is disabled on selected devices and the PHD collection status for the devices is changed to disabled.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Aborting a Product Health Data Collection Configuration on page 275](#)

- [Retrying Collecting Product Health Data from a Device on page 271](#)
- [Rescheduling a Product Health Data Collection Configuration on page 270](#)
- [Modifying a Product Health Data Collection Configuration on page 267](#)
- [Viewing Product Health Data Files Collected from a Device on page 256](#)

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 list, 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 87 on page 274](#).

The page lists the devices on which PHDC can be enabled.

Figure 87: 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.

On clicking Submit, Service Now displays a message indicating PHD collection is enabled on selected devices and the PHD collection status for the device is changed to enabled.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Aborting a Product Health Data Collection Configuration on page 275](#)
 - [Retrying Collecting Product Health Data from a Device on page 271](#)
 - [Rescheduling a Product Health Data Collection Configuration on page 270](#)
 - [Modifying a Product Health Data Collection Configuration on page 267](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)

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:

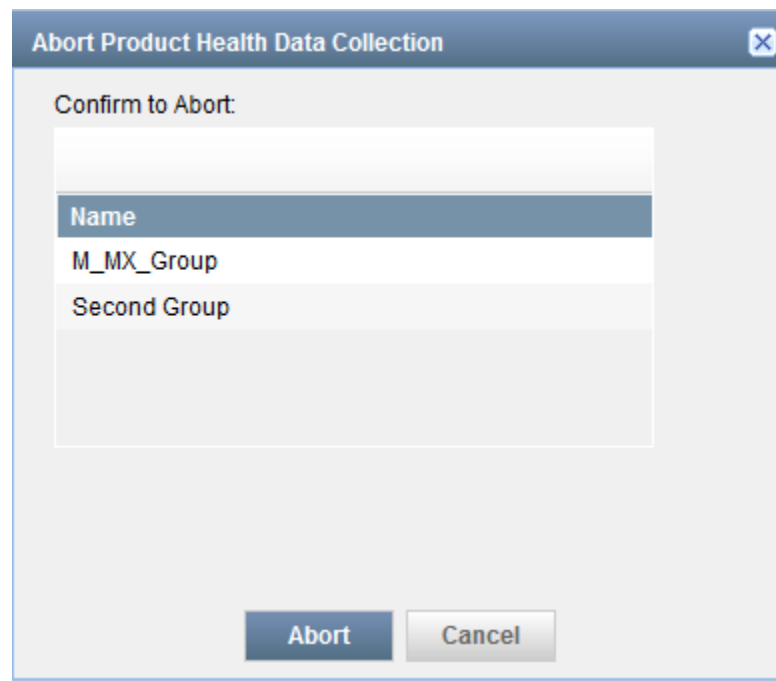
1. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

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 list, 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 88 on page 276](#).

Figure 88: Abort Product Health Data Collection Dialog Box



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

On clicking Submit, Service Now displays a message indicating that the PHDC configuration is successfully aborted and sets the status of the PHDC configuration and the PHD collection to aborted.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Disabling Product Health Data Collection on a Device on page 273](#)
 - [Enabling Product Health Data Collection on a Device on page 274](#)
 - [Retrying Collecting Product Health Data from a Device on page 271](#)
 - [Rescheduling a Product Health Data Collection Configuration on page 270](#)
 - [Modifying a Product Health Data Collection Configuration on page 267](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)

Exporting Product Health Data Information to an Excel File

Junos Space Service Now provides the Export and Export All options in the Actions list of the Product Health Data Devices page 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 89 on page 277 shows a sample of the information about devices exported to Excel.

Figure 89: 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	D4368	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 *yyyy-mm-dd* and *hhmmss* are the date and time the Excel file was created.

Figure 90 on page 277 shows a sample of the information about PHD files exported to Excel.

Figure 90: 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 01:18:03.25	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 277
- Exporting Data about PHD Files Collected from a Device on page 279

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, Service Now exports information about all the managed devices in Service Now from which PHD is collected; whereas, when you export information about devices from the Product Health Data Collection task in the Administration workspace Service Now exports, information about devices in the selected PHDC configuration.

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 91 on page 278](#). The View all Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 91: View all Devices of this PHDC

Device	Serial Number	Product	Start Date	Status	Total Files Available
snv-220-en1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snv-650-en2	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**.

Service Now displays the Export All Product Health Data Devices dialog box. 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**.

Service Now displays the Export Selected Product Health Data Devices dialog box. 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 92 on page 280](#).

Figure 92: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_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 93 on page 280](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 93: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
sr1-220-sr1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
sr1-650-sr2	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**.

Service Now displays the Export All Product Health Data Information dialog box. 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**.

Service Now displays the Export Selected Product Health Data Information dialog box. 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.

- See Also**
- [Service Now Product Health Data Collection Overview on page 254](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)

Deleting Product Health Data Files Collected from a Device

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

Service Now provides the Delete option to delete the PHD files if you choose to do so. 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 94 on page 282](#).

Figure 94: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

- To delete the PHD files from the Product Health Data Collection task of the Administration workspace:
 - 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 95 on page 282](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 95: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
sr1-220-sr1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
sr1-650-sr2	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 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, Service Now displays a message indicating that the files are deleted.

- See Also**
- [Service Now Product Health Data Collection Overview on page 254](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)
 - [Exporting Product Health Data Information to an Excel File on page 276](#)

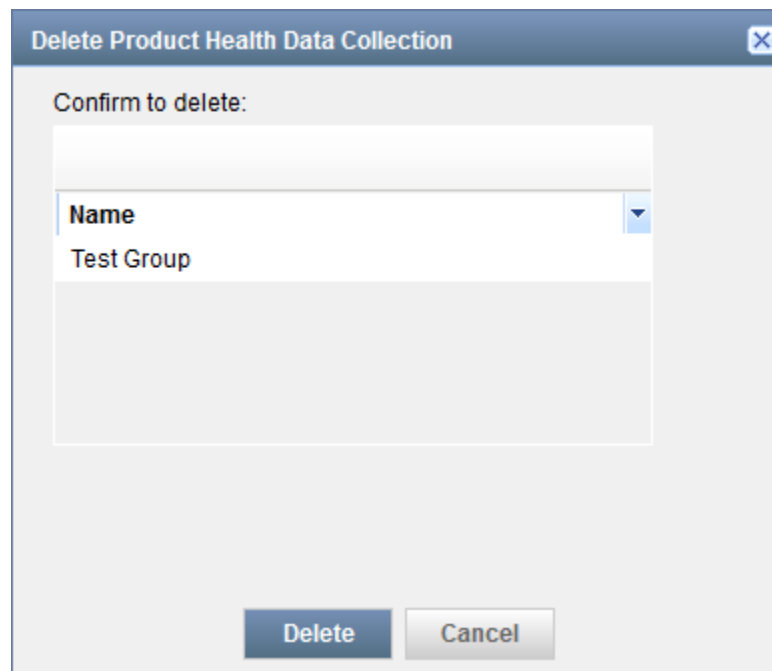
Deleting a Product Health Data Collection Configuration from Service Now

Service Now provides the Delete option on the Actions list to delete a PHDC configuration. You can delete a PHDC configuration 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 list, select **Delete**. Alternatively, right-click the PHDC configuration and select **Delete**.

The Delete Product Health Data Collection dialog box appears as shown in [Figure 96 on page 284](#).

Figure 96: View all Product Health Data Files PageA screenshot of a web-based dialog box titled "Delete Product Health Data Collection". The dialog has a blue header bar with a close button (X) in the top right corner. Below the header, the text "Confirm to delete:" is displayed. Underneath, there is a form area with a label "Name" and a dropdown menu showing "Test Group". At the bottom of the dialog, there are two buttons: "Delete" (in blue) and "Cancel" (in grey).

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

When you click Submit, Service Now displays a message indicating that the PHDC configuration is successfully deleted.

- See Also**
- [Product Health Data Collection Configuration Overview on page 259](#)
 - [Configuring Product Health Data Collection on a Device on page 262](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)
 - [Disabling Product Health Data Collection on a Device on page 273](#)
 - [Enabling Product Health Data Collection on a Device on page 274](#)
 - [Retrying Collecting Product Health Data from a Device on page 271](#)
 - [Rescheduling a Product Health Data Collection Configuration on page 270](#)
 - [Modifying a Product Health Data Collection Configuration on page 267](#)

Address Groups

- [Service Now Address Group Overview on page 285](#)
- [Creating an Address Group on page 286](#)
- [Modifying an Address Group on page 286](#)
- [Deleting Address Groups on page 287](#)

- [Associating Devices with an Address Group From the Address Groups Page](#) on page 287
- [Associating Devices with an Address Group From the Organizations Page](#) on page 289
- [Associating Devices with an Address Group from the Device Groups Page](#) on page 290
- [Associating Devices with an Address Group from the Service Now Devices Page](#) on page 292

Service Now Address Group Overview

Junos Space Service Now provides the Address Group task to configure addresses where devices are located and assign those addresses to devices. This address is used by Juniper Networks for shipping replacement parts and mail communications. You can view address groups configured on Service Now on the Address Groups page (**Administration > Address Group**).

A Service Now partner can use the partner address instead of end-customer address when submitting RMA cases for end customers to Juniper Support Systems (JSS). This can be done through a setting at the connected member and when submitting a case manually. For an auto submit 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 Networks.

You can associate devices to any of the address groups defined in the system. You can also associate devices to address group subtypes (Location, Ship- to, and Both) from the Organizations page, Device Groups page, and Devices page.

Associated Actions

You can perform the following actions related to address groups:

- View address groups configured in Service Now
- Create a new address group; see [“Creating an Address Group”](#) on page 286 for details.
- Modify an existing address group; see [“Modifying an Address Group”](#) on page 286 for details.
- Delete address groups; see [“Deleting Address Groups”](#) on page 287 for details.
- Associate address group to a set of devices; see [“Associating Devices with an Address Group From the Address Groups Page”](#) on page 287 for details.

- See Also**
- [Service Now Devices Overview](#) on page 117
 - [Service Now Organizations Overview](#) on page 99
 - [Service Now Device Groups Overview](#) on page 111
 - [Generating an RMA Incident for a Device](#) on page 142

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.

Address Group Name, Address1, City and Country are mandatory fields.

3. Click **Submit**.

Service Now creates the new address group and displays it on the Address Group page.

- See Also**
- [Service Now Address Group Overview on page 285](#)
 - [Modifying an Address Group on page 286](#)
 - [Deleting Address Groups on page 287](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 287](#)

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**.

Service Now modifies the address group. You can view the modified address on the Address Group page.

- See Also**
- [Service Now Address Group Overview on page 285](#)
 - [Creating an Address Group on page 286](#)
 - [Deleting Address Groups on page 287](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 287](#)

Deleting Address Groups

Junos Space Service Now provides the Delete option in the Actions list for the Address Groups page to delete address groups.

To delete address groups:

1. From the Service Now navigation tree, select **Administration** > **Address Group**. The Address Group page appears.
2. Select one or more 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.

Service Now deletes the selected address groups and removes them from the Address Groups page.

- See Also**
- [Service Now Address Group Overview on page 285](#)
 - [Creating an Address Group on page 286](#)
 - [Modifying an Address Group on page 286](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 287](#)

Associating Devices with an Address Group From the Address Groups Page

Junos Space Service Now provides the Associate Devices option in the Actions list of the Address Groups page to associate devices with address groups.

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 you want to associate 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 as shown in [Figure 97 on page 288](#).

Figure 97: Associate Address Group to Devices Page

Associate Address Group to Devices

Name: test
Address:
City: t
State: t
Country: t
Zip: t

Select Address Types

Location
Ship-to
Both

Associate or remove devices from Location

Hostname	Platform	Serial Number	Organization	Device Group
ex-2200-sn3	junos-ex	CW0210403356	ec	Device Group for ec
sn-space-ex4500-sys1	junos-ex	GG0213130986	ec	Device Group for ec
ex-4200-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

Page 1 of 1 | Showing 1 - 7 of 7 | Show 30 | It's

Close

You can associate devices to this address group in any of the following 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 replacement of a 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**.
Service Now assigns the address configured in the address group to the selected devices' as the 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.

- See Also**
- [Service Now Address Group Overview on page 285](#)
 - [Creating an Address Group on page 286](#)
 - [Modifying an Address Group on page 286](#)
 - [Deleting Address Groups on page 287](#)
 - [Associating Devices with an Address Group From the Organizations Page on page 289](#)
 - [Associating Devices with an Address Group from the Device Groups Page on page 290](#)
 - [Associating Devices with an Address Group from the Service Now Devices Page on page 292](#)

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 98: 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

- See Also**
- [Service Now Organizations Overview on page 99](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 287](#)
 - [Associating Devices with an Address Group from the Device Groups Page on page 290](#)
 - [Associating Devices with an Address Group from the Service Now Devices Page on page 292](#)

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 99 on page 291](#).

Figure 99: 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.

- See Also**
- [Service Now Device Groups Overview on page 111](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 287](#)
 - [Associating Devices with an Address Group From the Organizations Page on page 289](#)
 - [Associating Devices with an Address Group from the Service Now Devices Page on page 292](#)

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.

- See Also**
- [Service Now Devices Overview on page 117](#)
 - [Associating Devices with an Address Group From the Address Groups Page on page 287](#)
 - [Associating Devices with an Address Group From the Organizations Page on page 289](#)
 - [Associating Devices with an Address Group from the Device Groups Page on page 290](#)

E-mail Templates

- [Service Now E-Mail Templates Overview on page 293](#)
- [Viewing E-Mail Templates on page 296](#)
- [Modifying an E-Mail Template on page 297](#)

Service Now E-Mail Templates Overview

You can use Junos Space Service Now to send notifications to users about an event, when it occurs on a device, by e-mails. Service Now provides templates for these e-mails to be sent under various situations such as when an incident is created, case is created, case and incident are assigned to a user for resolution, or when the incident or case is closed. With administrator privileges, you can modify the content of an e-mail template. However, you cannot delete the default templates.

Service Now displays two types of templates: license-specific and generic e-mail templates based on the mode in which Service Now is operating. For example, if Service Now is operating in Direct mode, the Email Templates page lists templates relevant to Direct mode; If Service Now is working in Partner Proxy mode, the Email templates relevant to Partner Proxy mode are displayed, and so on.

Figure 100: E-Mail Templates Page

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 an 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

Table 28 on page 294 lists the e-mail templates provided by Service Now and the modes in which the templates can be used.



NOTE: Starting in Service Now Release 16.1R1, the following e-mail notifications include a five-digit ID of the incident and status of the case created for the incident:

- Incidents flagged to users
- Incidents submitted to JSS
- New incidents detected
- New iJMBs collected from devices

Starting with Service Now Release 17.2R1, the URL in the notification sent out by Service Now includes a fully qualified domain name (FQDN) of the Junos Space server where Service Now is installed instead of the IP address.

The following notifications have FQDN in the URLs:

- Incident Detected
- Incident Submitted
- Case ID Assigned
- Case Status Updated
- End Customer Incident Submitted in Partner Proxy
- End Customer Case Created in Partner Proxy
- End Customer Case Updated in Partner Proxy
- End Customer Case Closed in Partner Proxy

Table 28: List of E-Mail Templates Provided by Service Now and the Modes in which the Templates can be Used

Template Name	Partner Proxy Mode	End Customer Mode	Direct Mode	Offline Mode	Demo Mode
Connected member device added/removed	Yes				
Contract expiry info received	Yes	Yes	Yes		Yes
Devices not Sending Device Snapshot	Yes	Yes	Yes	Yes	Yes
End Customer Case Closed in Partner Proxy	Yes				
End Customer Case Created in Partner Proxy	Yes				
End Customer Case Updated in Partner Proxy	Yes				
End Customer Incident Submitted to Partner Proxy	Yes				
Incident Flagged to Users		Yes			

Table 28: List of E-Mail Templates Provided by Service Now and the Modes in which the Templates can be Used (continued)

Incident Submitted to Juniper by Partner Proxy	Yes				
Incident Submitted to Juniper Support Systems			Yes		Yes
Incident Submitted to Connected Junos Space Appliance		Yes			
Incomplete RAM Incident Submitted to Juniper	Yes		Yes		
Incomplete RAM Incident Submitted to Partner Proxy		Yes			
Juniper Technical Support Case Created for Incident from Partner Proxy	Yes				
Juniper Technical Support Case Created for Incident			Yes		Yes
Juniper Technical Support Case Updated	Yes		Yes		Yes
Case Created for Incident		Yes			
Case Updated		Yes			
Message Flagged to Users	Yes	Yes	Yes	Yes	Yes
New Exposure Info Received	Yes	Yes	Yes		Yes
New Incident Detected	Yes	Yes	Yes	Yes	Yes
New Intelligence Info Received	Yes	Yes	Yes		Yes
Ownership of Message Assigned to Users	Yes	Yes	Yes	Yes	
Ownership of Service Now Incident has been Assigned to User	Yes	Yes			Yes
Partner Certificate Expired	Yes	Yes	Yes		Yes
Partner Certificate Expiry	Yes	Yes	Yes		Yes
Product Health Data Collection Failure	Yes	Yes	Yes	Yes	Yes
Switch Over enabled for iJMB	Yes	Yes	Yes	Yes	Yes

Associated Actions

You can perform the following actions related to e-mail templates:

- View e-mail templates; see [“Viewing E-Mail Templates” on page 296](#) for details.

- Modify e-mail templates; see “Modifying an E-Mail Template” on page 297 for details.

- See Also**
- [Service Now Notification Policies Overview](#) on page 384
 - [Creating and Editing a Notification Policy](#) on page 386

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 as shown in [Figure 101](#) on page 296.

Figure 101: Email Templates Page

Name	Description	Created By	Last Updated
Connected member device added/removed	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST
Contract Expiry Info Received	This template is used by Service Now when sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
Devices Not Sending Device Snapshot	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
End Customer Case Closed in Partner Proxy	This email is sent when an end customer case (from a Service Now ...	Service Now	Jul 12, 2016 4:39:41 AM IST
End Customer Case Created in Partner Proxy	This email is sent when an end customer case (from a Service Now ...	Service Now	Jul 12, 2016 4:39:41 AM IST
End Customer Case Updated in Partner Proxy	This email is sent when an end customer case (from a Service Now ...	Service Now	Jul 12, 2016 4:39:41 AM IST
End Customer Incident Submitted to Partner Proxy	This email is sent when an case is submitted to the Service Now P...	Service Now	Jul 12, 2016 4:39:41 AM IST
Incident Flagged to Users	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST
Incident Submitted to Juniper by Partner Proxy	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
Incomplete RMA Incident Submitted to Juniper	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
Juniper Technical Support Case Created for Incident from Partner Proxy	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
Juniper Technical Support Case Updated	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST
Message Flagged to Users	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST
New Exposure Info Received	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
New Incident Detected	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
New Intelligence Info Received	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:41 AM IST
Ownership of Message Assigned to Users	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST
Ownership of Service Now Incident has been Assigned to User	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST
Partner certificate Expired	This template is used by Service Now when sending email ...	Service Now	Jul 12, 2016 4:39:42 AM IST
Partner certificate Expiry	This template is used by Service Now when sending email ...	Service Now	Jul 12, 2016 4:39:42 AM IST
Product Health Data Collection failure	This email is sent when Service Now fails to collect Product...	Service Now	Jul 12, 2016 4:39:42 AM IST
Switch over enabled for LMB	This template is used by Service Now for sending email notificat...	Service Now	Jul 12, 2016 4:39:42 AM IST

2. Double-click the required template from the list.

The Email Template Details page appears. The Email Template Details page displays the following information about an e-mail template:

- Name of the template
- Date and time the template was last updated
- Description of the template
- Subject of the e-mail template
- Information such as JTAC case ID, incident priority, incident ID, and synopsis that you can modify

- See Also**
- [Service Now E-Mail Templates Overview](#) on page 293
 - [Modifying an E-Mail Template](#) on page 297

Modifying an E-Mail Template

Service Now provides the Modify Email Template option on the Actions list of the Email Templates page to modify the contents of e-mail templates. An e-mail template for an end customer contains \$ variables and static content. You cannot modify the \$ variables, but you can remove them from the template. 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 a 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 the check box.

- See Also**
- [Service Now E-Mail Templates Overview on page 293](#)
 - [Viewing E-Mail Templates on page 296](#)

CHAPTER 7

Service Central

- [Service Central Overview on page 299](#)
- [Incidents on page 301](#)
- [Technical and End Customer Support Cases on page 326](#)
- [Collecting Additional Information for Incidents and Cases on page 333](#)
- [Information on page 352](#)
- [Device Analysis on page 363](#)
- [JMB Errors on page 378](#)
- [Suppressed Events on page 380](#)
- [Notifications on page 384](#)

Service Central Overview

The Service Central workspace of the Service Now application lets you to manage incidents, information messages, device snapshots, notifications, and error JMBs. 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. In response to the JMB received, Service Now creates a new incident for the JMB and displays it on the Incidents page.

The Service Central workspace displays the following three gadgets on its dashboard to display information about incidents graphically:

- Incident severities—Provides a graphical representation of the incidents generated and their severities.
- Incident priorities—Provides a graphical representation of the incidents generated and their severity.
- My Incidents—Provides a graphical representation of the newly created incidents, incidents flagged to you, or owned and changed by you.

When you click a bar on the graph, service Now takes you to the Incidents page listing only the incidents represented by the bar..

Figure 102: Service Central Gadgets



After viewing an incident, you can submit a case to the Juniper Support Systems (JSS) or a Service Now partner (in End Customer mode). 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.

Service Now considers a JMB 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 you can view or download them for analysis.

Service Now provides the notifications task in Service Central workspace to configure notification policies which define the conditions such as new incident is detected or a new incident is submitted, when service Now must send notifications to users. Notification policies also provide filters that you can use to fine tune the conditions under which you receive a notification.

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* in the [Junos Space Service Now Administration Guide](#).

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:

- **Manage incidents**—You can view, delete, export, submit to create a case, view JMB associated with the incident, and upload core files for the incidents.
- **Manage cases**—You can view the technical support cases that were created for incidents you submitted, collect additional information for the cases, update case with additional notes, and upload attachments for the case.

If Service Now is operating in the Partner Proxy mode, you can view and manage cases for your end customers (also known as connected members).

- **Manage messages and notifications from JSS**—You can view and assign or flag informational messages that you receive from JSS or Service Now partner to specific users.
- **Manage device snapshots (also known as informational JMBs or iJMBs)**—You can view, export the JMB information to an HTML file and delete the iJMBs.
- **View and export BIOS validation data collected from devices**
- **View and export product health data collected from devices**
- **View and download erroneous JMBs**
- **View JMBs for which Service Now did not create incidents**
- **Manage notifications**—You can create, enable or disable and copy notifications information about devices that are susceptible to known issues.

Related Documentation

- [Junos Space Service Now Overview on page 54](#)
- [Service Now Modes](#)
- [Service Now Incidents Overview on page 302](#)
- [Service Now Device Snapshots Overview on page 357](#)
- [Service Now Messages Overview on page 353](#)
- [JMBs with Errors on page 378](#)
- [Service Now Notification Policies Overview on page 384](#)
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 326](#)
- [Service Now Suppressed Events Overview on page 380](#)

Incidents

- [Service Now Incidents Overview on page 302](#)
- [Assigning an Owner to an Incident on page 305](#)

- [Flagging an Incident to a User on page 306](#)
- [Checking Incident Status Updates on page 307](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
- [Deleting an Incident on page 310](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
- [Viewing Incident Details on page 316](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
- [Uploading an Attachment to an Incident on page 320](#)
- [Updating an End-Customer Case on page 322](#)
- [Uploading Core Files to JSS for an Incident on page 323](#)
- [Associating an Incident with an Existing Case on page 324](#)

Service Now Incidents Overview

Junos Space Service Now generates an incident and lists it on the Incidents page (at **Service Central > Incidents**) when a Juniper Message Bundle (JMB) is received. 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 JMB 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. Service Now displays the incidents created on the Incidents page chronologically, by organization name, and by device group. 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. For information about notifications, see [“Service Now Notification Policies Overview” on page 384](#).

[Table 29 on page 302](#) lists the fields on the Incidents page.

Table 29: 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
Connected Member	

Table 29: Fields on the Incidents Page (continued)

Fields	Description
Priority	<p>The priority of the incident</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 1-Critical • 2-High • 3-Medium • 4-Low
Type	The type of defect
Problem Identifier	The ID of the incident
Remarks	Remarks, If any, about errors while reading the JMB, creating the incident, or uploading the incident to Juniper Support Systems (JSS).
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 to which the device belongs
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	<p>The status of the incident</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Not Submitted—Incident is not submitted to JSS. • Submitted—Incident is submitted to JSS. • Created—A case is created for the incident and an ID is assigned to the case in JSS. • Updated—The case ID of the incident is updated in JSS. • Create Failed—A case could not be created in JSS for the incident. • Closed—The case is closed in JSS. • Submission Failed—The incident could not be submitted to JSS for creating a case. • Associated to a Case—The incident is associated with a case.

Table 29: Fields on the Incidents Page (continued)

Fields	Description
Flagged	Specifies whether the incident is lagged to you. Possible values: <ul style="list-style-type: none"> • Yes—The incident is flagged to you. • No—The incident is not flagged to you..
Entity	The entity of the device for which the incident was created; for example, Routing Engine (re0, re1), power supply, and FPCs



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).

Associated Actions

You can perform the following actions related to incidents:

- Export JMB to HTML; see [“Exporting a Juniper Message Bundle \(JMB\) to an HTML file” on page 308](#) for details.
- Delete an incident; see [“Deleting an Incident” on page 310](#) 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 319](#) for details.
- View a case in the Juniper Networks Case Manager; see [“Viewing a Case in Case Manager” on page 330](#) for details.
- Assign an incident to a user; see [“Assigning an Owner to an Incident” on page 305](#) for details.
- Flag an incident to a user; see [“Flagging an Incident to a User” on page 306](#) for details.
- Submit an incident to create a JTAC case; see [“Submitting an Incident to Juniper Support Systems or Service Now Partner” on page 311](#) for details.
- Export the summary of an incident to Excel; see for details.
- Update an end customer case; see [“Updating an End-Customer Case” on page 322](#) for details.
- Create auto submit policy for an incident; see [“Creating an Auto Submit Policy” on page 243](#) for details.
- Upload core files to JSS for incidents; see [“Uploading Core Files to JSS for an Incident” on page 323](#) for details.

- Upload attachments; see [“Uploading an Attachment to an Incident” on page 320](#) for details.
- Associate an incident with a case; see [“Associating an Incident with an Existing Case” on page 324](#) for details.



NOTE: From Service Now Release 17.1R1, you can associate an incident with a case which is in the open state.

- Configure Junos OS commands for collecting additional information for an incident; see [“Collecting Additional Information for Service Now Incidents and Cases Overview” on page 334](#) for details.



NOTE: From Service Now Release 17.1R1, you can configure Junos OS commands for collecting information, in addition to the information provided by a JMB, for an incident.

- See Also**
- [Service Now Auto Submit Policy Overview on page 241](#)
 - [Service Now Devices Overview on page 117](#)
 - [Service Now Notification Policies Overview on page 384](#)


Assigning an Owner to an Incident

Junos Space Service Now provides the Assign Ownership option on the Actions list of the Incidents page to assign a user to look into the incident. The owner tracks the progress of the related case and the updates from JSS.

To assign an incident to a Service Now user:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select the incident to which you want to assign an owner, and select **Assign Ownership** from either the **Actions** list or the right-click menu.

The **Assign Ownership** dialog box appears.

The image shows a dialog box titled "Assign Ownership" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Enter the Login ID of User" with a text input field containing the word "super" and a search icon (magnifying glass) to its right. Below this, there is a checked checkbox labeled "Email Incident to Assigned Owner". At the bottom of the dialog, there are two buttons: "Submit" and "Cancel".

3. Enter the login ID of the Service Now 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**.
Service Now assigns the incident to the specified user. .

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Deleting an Incident on page 310](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Viewing Incident Details on page 316](#)
 - [Viewing a Case in Case Manager on page 330](#)
 - [Updating an End-Customer Case on page 322](#)

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 page 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**.
Service Now sends an e-mail notification for the incident to all the selected users.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Deleting an Incident on page 310](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Viewing Incident Details on page 316](#)
 - [Viewing a Case in Case Manager on page 330](#)
 - [Updating an End-Customer Case on page 322](#)

Checking Incident Status Updates

You can use the Incidents page to submit an incident to JSS or Service Now partner 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 the following 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 386](#).
- 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 you last logged in.

To view the graphs on the Service Central page, click **Service Central** from the Service Now navigation tree.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
 - [Deleting an Incident on page 310](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Viewing Incident Details on page 316](#)
 - [Viewing a Case in Case Manager on page 330](#)
 - [Updating an End-Customer Case on page 322](#)
 - [Associating an Incident with an Existing Case on page 324](#)

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

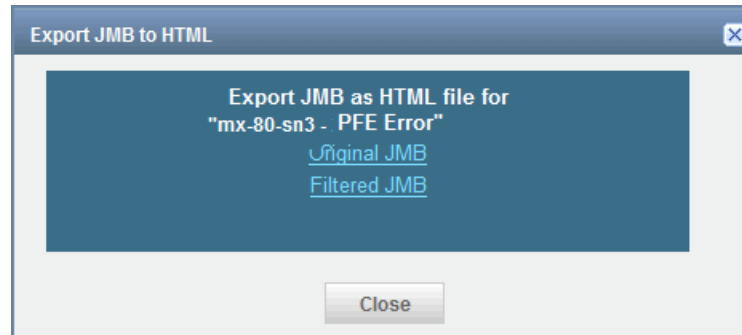
Junos Space Service Now provides the Export JMB to HTML option in the Actions list to export JMB data along with its attachments as HTML files and save them on your local file system. A JMB is exported as a zipped folder. Logs are not exported. The view of the exported JMB file is the same as of the View JMB page in Service Now. However, the option to download the attachments and log files is not available for an exported JMB file.

To export a JMB 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 for which you want to export JMB
3. From the Actions list, 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 103 on page 309](#).

Figure 103: Export JMB to HTML Dialog Box



4. Click the **Original JMB** or **Filtered JMB** link to save or open the original or filtered JMB file as an HTML file.
5. The browser opens the dialog box to save or open the JMB file.
Click **Save** to save the JMB as an HTML file or **Open** to open the JMB 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.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Deleting an Incident on page 310](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)

- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
- [Viewing Incident Details on page 316](#)
- [Viewing a Case in Case Manager on page 330](#)
- [Updating an End-Customer Case on page 322](#)

Deleting an Incident

Junos Space Service Now provides the Delete action in the Actions list of the Incidents page to delete incidents.

Service Now provides the Submitted Incident Purge Time and Not Submitted Incident Purge Time parameters in global settings to configure the number of days after which incidents that are submitted or incidents that are not submitted can be deleted automatically from the Service Now database. The Delete option provides you the flexibility to delete incidents whenever you want to delete before the configured purge time.

To delete incidents:

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

The Incidents table appears.

2. Select one or more incidents that you want to delete.

3. Click **Delete**.

The selected incidents are removed from the Incidents table and the Service Now database.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Viewing Incident Details on page 316](#)
 - [Viewing a Case in Case Manager on page 330](#)
 - [Updating an End-Customer Case on page 322](#)

Submitting an Incident to Juniper Support Systems or Service Now Partner

Junos Space Service Now provides the Submit Case option in the Actions list of the incidents page to submit an incident to Juniper Support Systems (JSS) or Service Now partner (in End Customer mode) for creating a case. After you submit an incident, Service Now changes the incident status to Submitted. For Service Now operating in the End Customer mode, the incident is submitted to the Service Now partner. The Service Now partner can submit the incident from the end customer to JSS.

If you have an auto submit policy configured to submit an incident for opening a case, Service Now submits the incident immediately after the incident is created. Starting with Service Now Release 17.2R1, Service Now provides the option *Minimum Incident Submission Delay Time (In Mins)* for configuring the time after which the incident should be submitted for creating a case. By configuring a time to delay submitting an incident, you can choose not to submit the incident until the time delay.



NOTE: Service Now displays the Submitted status in red if an error or exception has occurred while submitting the incident to JSS or Service Now partner. 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:

- *Event* indicates the incident was generated due to an event in a device.
- *On Demand* indicates on-demand incidents generated by Service Now
- *Event RMA* indicates RMA incidents detected by AI-Scripts
- *Event (low end)* indicates
- *On Demand RMA* indicates 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. Service Now automatically uploads the JMB attachments to the related case after collecting them from the device.

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 list, select **Submit Case**. Alternatively, right-click the incident and select **Submit Case**.

Figure 104 on page 312 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 104: 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.



NOTE: Site ID and User Name can be modified only if Service Now is operating in the Direct or Partner Proxy mode. In End Customer mode, Site ID and Username fields are not visible on the Submit Case Options page.

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
 - c. (Optional) Select the **Save As Default User For Incident Submission** check box if you want to submit incidents for that site only for the selected user .
 - For a new user:
 - a. Click **User Name**.
 - b. 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.
 - c. In the **Password** field, enter the password to log in to the organization.
The password is provided by Juniper Networks.
 - d. Click the **Get Sites** link.
The Site ID list displays a list of site IDs associated with the user name.
 - e. 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 Direct, 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. If needed, you can create a new address group and associate it with the device or you can select any other configured address group for creating a case.
- For an end-customer device, in the Partner Proxy mode, the Address Group and Ship-to Address fields are prepopulated with the address group sent by the end-customer and the address group present in the system for opening a case. The Service Now partner has the option of changing this value to an address group present in their system.
- If the Service Now 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 address provided by the end-customer.
- If a device is not associated with an address group, None is displayed in the Address Group field for that device.

The address group selected on the Submit Case page is submitted as the shipping address to the Service Now partner.

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 text or 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 mode.

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) In the **Minimum Incident Submission Delay Time (In Mins)** field enter the number of minutes by which you want Service Now to delay submitting the incident for creating a case.

You can delay submitting an incident by 1 – 21600 minutes.

14. (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.

15. (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

16. Select one or more core files to upload.

The core files are uploaded after the case is created for the incident.

17. (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.

18. (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.

19. Select the device components for which you want to request RMA incidents and click **Submit**.

20. In the **Problem Description** field, enter information about the device components (part number, version, part description, part serial number, and so on).

21. 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.

22. Navigate back to **Service Central > Incidents**.

The Incidents page appears.

23. 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.

24. 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.

25. 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.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Viewing Incident Details on page 316](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
 - [Viewing a Case in Case Manager on page 330](#)
 - [Updating an End-Customer Case on page 322](#)

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.
- Collect Additional Information Attachment Details tab: Provides details about the information collected for an incident in addition to information provided by JMBs. The additional information is collected by executing Junos OS commands on devices by a user.



NOTE: Starting Service Now Release 17.1R1, the Collect Additional Information Attachment Details tab is displayed on the Incident Detail page to provide details about the information collected in addition to information provided by JMBs.

To view details of an incident:

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 Incident 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, Log File Details, and Collect Additional Information Attachment Details tab as shown in [Figure 105 on page 318](#). The **End-Customer Case Details** tab appears in the partner proxy mode for end customer incidents.

Figure 105: Incident Detail Page

The screenshot shows the 'Incident Detail' window with the following tabs: Incident Details (selected), Case Details, Core File Details, Attachment Details, Log File Details, and Collect Additional Information Attachment Details. The main content area displays the following information:

- Device: sn-space-ex4550-sys
- IP Address: 10.219.30.157
- Device Serial Number: LX0213163855
- Product: EX4550-32F
- Platform: junos-ex
- Release: 15.1R5.5
- Organization: Prod_Org
- Device Group: Default for TestORG
- Connected Member:
- Occurred: May 26, 2017 1:48:45 PM IST
- Status: Case Associated, 2017-0526-0673
- Problem Identifier: sn-space-ex4550-sys-279-20170526-081843-279
- Event Type: Software Failure
- Defect Type: File system error
- Entity: re0
- Job Id: ---
- Filter Name:
- KB Article: <http://kb.juniper.net/InfoCenter/index?page=content&actp=SN&id=KB18770>

An 'OK' button is located at the bottom right of the window.

You can retrieve required information from the tabs.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)

- [Flagging an Incident to a User on page 306](#)
- [Deleting an Incident on page 310](#)
- [Checking Incident Status Updates on page 307](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 319](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
- [Viewing a Case in Case Manager on page 330](#)
- [Updating an End-Customer Case on page 322](#)
- [Troubleshooting Issues with Creating Incidents](#)
- [Associating an Incident with an Existing Case on page 324](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)

Viewing Knowledge Base Articles Associated with an Incident

A Knowledge Base (KB) article provides information about the causes and solutions for a problem. Junos Space Service Now provides the View KB Article in the Actions list to 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 for which you want to view the KB article 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 KB articles.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Deleting an Incident on page 310](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)

- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
- [Viewing Incident Details on page 316](#)
- [Viewing a Case in Case Manager on page 330](#)
- [Updating an End-Customer Case on page 322](#)

Uploading an Attachment to an Incident

Junos Space Service Now provides the Upload Attachment option on the Actions list 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.

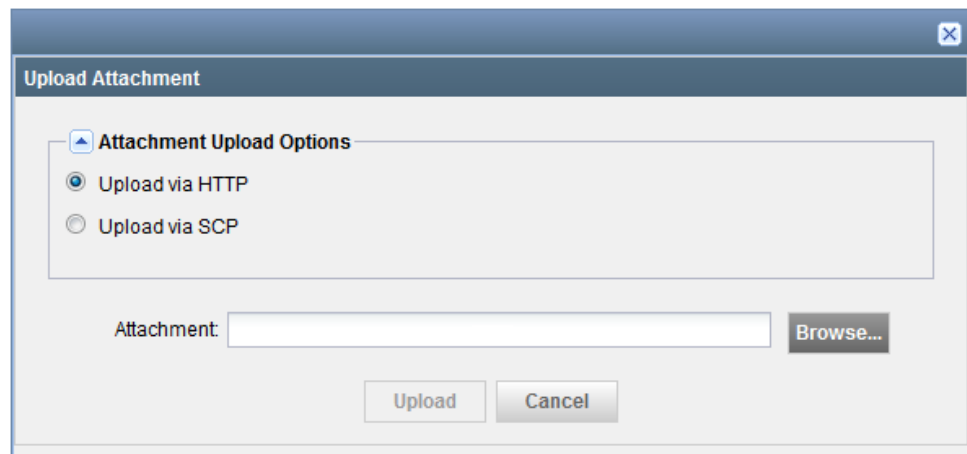
The attachment is stored in Service Now if the incident is not submitted to JSS. If a case is already created for the incident, the attachment, when uploaded to the incident is automatically uploaded to the case as well. An attachment that is uploaded to Service Now can be viewed on the View JMB page 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 list, select **Upload Attachments**. Alternatively, right-click the incident and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in figure.

Figure 106: Upload Attachment Dialog Box



4. Under Attachment Upload Options, select an option to upload an attachment as follows:

- 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**.

Service Now initiates the upload of the attachment and displays the File Upload Job information dialog box.

After the upload job is complete, you can view the attachment in the JMB associated with the incident.

- See Also**
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 326](#)
 - [Service Now Incidents Overview on page 302](#)
 - [Uploading an Attachment to a Case on page 331](#)

Updating an End-Customer Case

In Partner Proxy mode, Junos Space Service Now provides the End Customer Cases option to submit an end-customer incident to create a case



NOTE: This action is enabled only when the status of the end-customer 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 107 on page 322](#).

Figure 107: End-Customer Cases Dialog Box

End Customer Cases

Case ID: ECC1

Case Link:

Case Status:

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.

- See Also**
- [Junos Space Service Now Overview on page 54](#)
 - [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 104](#)
 - [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Deleting an Incident on page 310](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Viewing Incident Details on page 316](#)
 - [Viewing a Case in Case Manager on page 330](#)

Uploading Core Files to JSS for an Incident

Junos Space Service Now provides the Upload Core Files option in the Actions list to upload core files generated for an event to Juniper Support Systems (JSS) or Service Now Partner. This option is enabled only when there is at least one core file available for upload.

- Case should be created for the incident
- At least one core file should be available for upload

When an end customer uploads core files, the core files are uploaded to the SFTP server configured by the Service Now partner. The Service Now partner provides the ID of the case for the incident submitted by the end customer. The case ID provided by the Service Now partner can be an ID created internally by the Service Now partner or created by JSS. In either case, the core files are uploaded automatically to the SFTP server once a case is created.

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.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Configuring SFTP Server for Uploading Core Files Generated for Events on page 198](#)
 - [Updating Core File Upload Configuration for an End Customer on page 110](#)

Associating an Incident with an Existing Case

Starting Junos Space Service Now Release 17.1R1, you can associate a new incident with technical support cases that are not closed. When you associate an incident with a case, the status of the incident on the Incidents page is set to **Case Associated** along with the **ID** of the case with which the incident is associated. You can also view the ID of the case with which the incident is associated on the Case Details tab of the Incident Details page. The attachments and log files of the incident are uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode) and associated with the related case.



NOTE:

- To associate an incident with a case, the case should not be in the Closed state.
- An incident created for a BIOS JMB cannot be associated with a case.
- Once an incident is associated with a case, the association cannot be undone.
- An incident in one domain can be associated with a case assigned to another domain. A case can be associated with multiple domains.
- When an incident (I1) is associated with a case that is created by submitting another incident (I2), the incident I1 is deleted or purged when incident I2 is deleted or purged.

To associate a new incident with an existing case:

1. In the Service Now navigation tree, click **Service Central > Incidents**.

The Incidents page appears.

2. Select an incident that you want to associate with an existing case.

3. Select **Associate Case** from the Actions list or the right-click menu.

The Associate Case ID page appears as shown in [Figure 108 on page 325](#).

Figure 108: Associate Case ID Page

4. In the **Case Id** text field, enter the Case ID with which you want to associate the incident.



NOTE: To associate an incident with a case, the case should be listed in the Technical Support Cases page and the status should not be Closed.

5. (Optional) Enter a comment when you associate the selected incidents with the case in the **Customer Comment** text field.

The incident information together with the customer comment appear as case notes (incident information listed first followed by the customer comment) in Case Manager. Total number of characters allowed in a case note is (incident information and customer comment) is 39000.

6. Click **Submit** to associate the selected incidents with the case.

Service Now associates the incidents with the case and sends the incident information and customer comments to Case Manager as case notes.

You can verify whether or not the incident is associated with a case by checking the status of the incident on the Incidents page (Service Central > Incidents). The status of the incident should be **Case Associated** along with the **case ID**.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Service Now Technical Support Cases and End Customer Support Cases Overview on page 326](#)
 - [Viewing Incident Details on page 316](#)
 - [Checking Incident Status Updates on page 307](#)

Technical and End Customer Support Cases

- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 326](#)
- [Viewing a Case in Case Manager on page 330](#)
- [Uploading an Attachment to a Case on page 331](#)

Service Now Technical Support Cases 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 Systems (JSS) and a case ID is assigned to the incidents. You can view the technical support cases on the View Tech Support page (**Service Central > Tech Support Case**) of the Service Central workspace.



NOTE: Technical support cases cannot be created when Service Now is operating in Demo mode or Offline 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.

Starting in Service Now Release 15.1R1, the Site ID and Device Name columns are provided on the View Tech Support Cases page when Service Now is operating in Partner Proxy and Direct modes to allow filtering cases based on site ID and device name. On the View End Customer Cases page, the Device Name column is provided to filter end-customer cases based on device name.

[Figure 109 on page 327](#) shows the View Technical Support Cases page.

Figure 109: 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 8:28:06 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0006	CABV4435	Aug 3, 2014 10:19:48 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0724-0010	CABV4435	Jul 24, 2014 3:24:43 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0803-0008	CABV4435	Aug 4, 2014 6:33:06 AM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0724-0017	CABV4435	Jul 24, 2014 5:14:07 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0317	CABV4435	Aug 1, 2014 4:42:52 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0801-0318	CABV4435	Aug 1, 2014 4:43:00 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0725-0050	CABV4435	Jul 25, 2014 5:18:08 PM IST		Other	2 - High	Open-Initial C
TestOrg	99248		2014-0727-0010	CABV4435	Jul 28, 2014 10:15:14 AM IST		Other	2 - High	Open-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

Starting in Service Now Release 16.1R1, the Case Details page of a Service Now partner displays case notes for the Service Now partner and End Customer Service Now on different tabs.

Table 30 on page 327 lists the columns displayed on the View Tech Support Cases page:

Table 30: 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 the 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

Table 30: Fields on the View Tech Support Cases Page (continued)

Field	Description
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
Priority	<p>Priority of the case.</p> <p>Possible values are:</p> <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 (**Service Central > View End Customer Cases**) of the Service Central workspace. The Service Now partner updates the status of the case to the Service Now end customer.

Figure 110 on page 328 shows the View End Customer Cases page.

Figure 110: View End Customer Cases Page

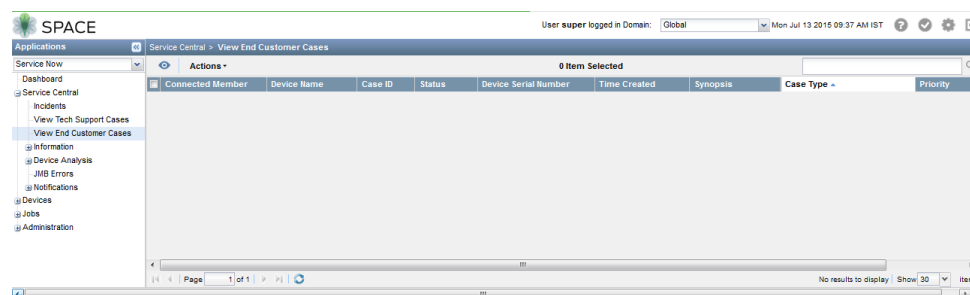


Table 31 on page 329 lists the columns displayed on the View End Customer Cases page:

Table 31: 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
Priority	<p>Priority assigned to the incident, by the end customer, for whom the case is created</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2- High • 3 - Medium • 4 - Low

Associated Actions

You can perform the following tasks related to tech support and end-customer cases:

- View details of a technical support case in Case Manager; see [“Viewing a Case in Case Manager” on page 330](#) for details.
- Add notes to a technical support case; see *Adding Notes to a Technical Support Case* for details.

- Upload binary or text attachments for a technical support case; see “[Uploading an Attachment to a Case](#)” on page 331 for details.
- Configure Junos OS commands for collecting additional information for a case; see “[Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case](#)” on page 345 for details.
- Update an end-customer support case; “[Updating an End-Customer Case](#)” on page 322 for details.
- View details of an end-customer case in Case Manager; see “[Viewing a Case in Case Manager](#)” on page 330 for details.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Service Now Notification Policies Overview on page 384](#)
 - [Service Now Organizations Overview on page 99](#)
 - [Junos Space Service Now Global Settings Overview](#)

Viewing a Case in Case Manager

You can view the details of a case submitted to JSS or Service Now partner 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 for a user ID and password at <https://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.

You can view a case in Case Manager by using Service Now in the following two ways—By using the Incidents task or by using the View Tech Support Case or View End Customer Case task

To view a case in Case Manager:

1. From the Service Now navigation tree, select **Service Central > Incidents**. The Incidents page appears.

Alternatively, you can also select **Service Central > View Tech Support Cases..**

The View Tech Support Cases page appears.

In a Service Now operating in Partner Proxy mode, if you want to view an end-customer case in Case Manager, select **Service Central > View End Support Cases**.

The View End Customer Cases page appears.

2. On the Incidents page, select the incident for which you want to view details of the associated case in the Case Manager, and select **View Case in Case Manager** from either the **Actions** list or the right-click menu.



NOTE: If the **View Case in Case Manager** link is not enabled on the Incidents page, verify whether a case is created for the incident.

On the View Tech Support Cases or View End Customer Cases page, select the case that you want to view in 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.

3. Enter your username and password and click **Login**.

The JSS Case Manager displays the case details.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Assigning an Owner to an Incident on page 305](#)
 - [Flagging an Incident to a User on page 306](#)
 - [Deleting an Incident on page 310](#)
 - [Checking Incident Status Updates on page 307](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 308](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 311](#)
 - [Viewing Incident Details on page 316](#)
 - [Updating an End-Customer Case on page 322](#)

Uploading an Attachment to a Case

Service Now provides the Upload Attachment option in the Actions list to upload a file, for example, a text, image, or binary file, as an attachment to a case created in Juniper Support Systems (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. However, attachments uploaded by an end customer are stored in Service Now partner.



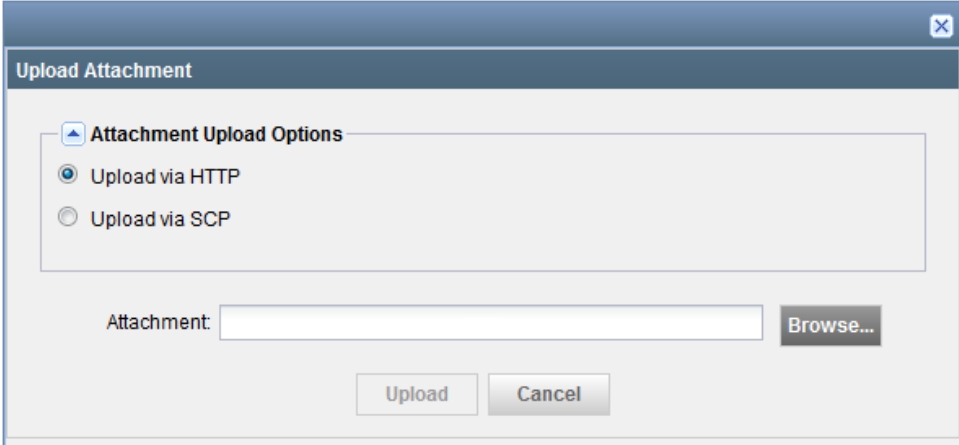
NOTE: We recommend that you limit the size of an attachment to be uploaded to 1 GB and use Secure Copy Protocol (SCP) to upload files of size 1 GB.

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 list, select **Upload Attachments**. Alternatively, right-click the case and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in [Figure 111 on page 332](#).

Figure 111: 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 from which you want to upload the attachment.
 - **Software File Path:** Specify the file path to access the Service Now image file on the local machine.
- c. Click **Submit**.

Service Now starts uploading the attachment and the File Upload Job dialog box displays the progress of the upload job. Close the dialog box after the job is complete.

- See Also**
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 326](#)
 - [Service Now Incidents Overview on page 302](#)
 - [Uploading an Attachment to an Incident on page 320](#)

Collecting Additional Information for Incidents and Cases

- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)
- [Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident on page 335](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
- [Modifying the Settings for Collecting Additional Information for an Incident on page 339](#)
- [Deleting the Settings for Collecting Additional Information for an Incident on page 341](#)
- [Downloading the Additional Information Collected About an Incident on page 342](#)
- [Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case on page 344](#)
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 345](#)
- [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 348](#)
- [Downloading the Additional Information Collected for a Technical Support Case on page 350](#)
- [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 351](#)

Collecting Additional Information for Service Now Incidents and Cases Overview

Starting in Junos Space Service Now Release 17.1R1, for an incident (**Service Central > Incidents**) or a technical support case (**Service Central > View Technical Support Case**), you can collect information in addition to what is available in a Juniper Message Bundle (JMB) by executing Junos OS commands on the device for which the incident and case are created. The additional information can be collected for an incident either before submitting the incident for opening a case or after the case is created. If a case is already created for the incident, the additional information collected can be directly uploaded to Juniper Support Systems (JSS) and associated with the case.

You can define the commands that can be executed to collect the additional information and the intervals at which the commands should be executed.

The additional information is collected from the device as a text file with the name **additional_cli_information_<devicename>_<timestamp>.txt** and associated with the incident in the Service Now database or uploaded to JSS if a technical support case is already created for the incident. If you are collecting additional information for a case, Service Now uploads the information directly to JSS from the device. For Service Now operating in the End Customer mode, the additional information is uploaded to the Service Now partner from where it is uploaded to JSS, if required.



NOTE:

- A Service Now partner cannot configure commands for collecting additional information for incidents or cases for its end customers.
 - Additional information cannot be collected for incidents and cases that are in the closed state.
-

Associated Actions

You can perform the following actions related to collecting additional information for an incident or case:

- Configure Junos OS commands to collect information for an incident; see [“Configuring Junos OS Commands to Collect Additional Information About an Incident” on page 336](#) for details.
- View Junos OS commands configured to collect information; see [“Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident” on page 335](#) for details.
- Modify Junos OS commands configured to collect information for an incident; see [“Modifying the Settings for Collecting Additional Information for an Incident” on page 339](#) for details.
- Delete Junos OS commands configured for collecting information for a case; see [“Deleting the Settings for Collecting Additional Information for an Incident” on page 341](#) for details.

- Download information collected for an incident; see [“Downloading the Additional Information Collected About an Incident”](#) on page 342 for details.
- View Junos OS commands configured for collecting additional information for a technical support case; see [“Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case”](#) on page 344 for details.
- Configure Junos OS commands configured for collecting additional information for a technical support case; see [“Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case”](#) on page 345 for details.
- Modify Junos OS commands configured for collecting additional information for a technical support case; see [“Modifying the Configuration for Collecting Additional Information for a Technical Support Case”](#) on page 348 for details.
- Delete Junos OS commands configured for collecting additional information for a technical support case; see [“Deleting the Configuration for Collecting Additional Information for a Technical Support Case”](#) on page 351 for details.
- Download Junos OS commands configured for collecting additional information for a technical support case; see [“Downloading the Additional Information Collected for a Technical Support Case”](#) on page 350 for details.

- See Also**
- [Service Now Technical Support Cases and End Customer Support Cases Overview](#) on page 326
 - [Service Now Incidents Overview](#) on page 302

Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident

You can view the Junos OS commands that are configured for collecting additional information about an incident on the Collect Additional Information Jobs Results Summary page. The Collect Additional Information Jobs Results Summary page displays the following information:

- Commands that are executed to collect additional information
- Name of the text file in which the command outputs are collected
- Status of the command execution
- Date and time the information was collected or is scheduled to be collected
- Job ID for executing the command
- User who configured the command
- Whether or not commands should be executed recurrently
- Remarks, if any, to indicate any issues that might have occurred while the commands for collecting additional information are executed

[Figure 112 on page 336](#) shows the Collect Additional Information Jobs Results Summary page.

Figure 112: Collect Additional Information Jobs Results Summary page

Collect Additional Information Jobs Result Summary							
Back							
Commands	File Name	Job Status	Scheduled Time	Job Id	Owner	Recurrence	Remarks
<input type="checkbox"/> show version	---	Scheduled	May 21, 2017 6:20:41 PM IST	1348115	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550- sys_20170521-124843926. txt	Success	May 21, 2017 6:18:41 PM IST	1348113	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550- sys_20170521-124643891. txt	Success	May 21, 2017 6:16:41 PM IST	1348111	super	Every 2 minutes First Occurrence: 2017-05-21 12:46:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550- sys_20170521-124444786. txt	Success	May 21, 2017 6:14:41 PM IST	1348109	super	Every 2 minutes First Occurrence: 2017-05-21 12:44:41.434	

To view Junos OS commands that are configured for collecting additional information for an incident:

1. From the Service Now Navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select the incident for which you want to view the commands configured for collecting additional information.
3. Select **Collect Additional Information > View** from the Actions list or the right-click menu.

The Collect Additional Information Jobs Results Summary page appears. The commands column lists the commands executed for collecting additional information and the Status column indicates whether the commands were executed successfully or not.

- See Also**
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
 - [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
 - [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 345](#)

Configuring Junos OS Commands to Collect Additional Information About an Incident

From Junos Space Service Now Release 17.1R1, in addition to the information provided by a JMB for an incident, you can configure Junos OS commands on the Incidents page for collecting additional information about the incident. When you configure commands to collect additional information, the commands you entered are executed on the device and the output is saved in a *.txt file and uploaded to the Service Now database. If a case is already created for the incident, the file is directly uploaded to Juniper Support Systems (JSS) or a Service Now partner (in case of End Customer mode).

**NOTE:**

- A Service Now partner cannot configure commands for collecting additional information about incidents or cases for its end customers.
- You cannot configure commands for collecting additional information for BIOS incidents and incidents that are closed.

To collect additional information about an incident by executing Junos OS commands:

1. From the Service Now Navigation tree, select **Service Central > Incidents**.

The Incidents page appears.

2. Select the incident about which you want to collect additional information.

3. Select **Collect Additional Information > Create** from the Actions list or the right-click menu.

The Collect Additional Information page appears as shown in [Figure 113 on page 337](#).

Figure 113: Collect Additional Information Page

Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: Multiple commands should be entered as , or ; or new line character.

☒ **Schedule at a later time**
 Start: 05/21/17 6:25 PM IST

☒ **Repeat**
 Interval: Weekly Every 1 Weeks
☒ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

Ends on: ☒ Never 05/21/17 6:25 PM IST

Submit Cancel

4. In the CLI Commands text box, enter the commands for collecting additional information



NOTE: Service Now does not validate the commands that you enter for collecting additional information. To add multiple commands, use comma (,) or semi-colon (;) or the new line character (press Enter on keyboard) consistently as the delimiter.

5. (Optional) Select the **Schedule at a later time** check box and select the date and time when you want the commands to be executed.



NOTE: Service Now executes the commands immediately if you do not schedule a date and time for the commands to be executed.

6. (Optional) Select the **Repeat** check box and select the time interval and the frequency of executing the commands.

You can select the intervals in minutes, hours, daily, weekly, monthly, or yearly to collect additional information. By default, an interval of once a week is selected.

7. (Optional) To define an end time for collecting information for the incident, do one of the following task:

- Click **Never** to continue collecting information by executing the commands at the defined interval until the incident is closed. This option is selected by default.
- Select the date and time when the commands should stop executing.

8. Click **Submit** to save the configuration or **Cancel** to cancel the configuration.

Service Now collects additional information immediately if the Schedule at a later time check box is not selected.

See "[Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident](#)" on page 335 to check whether the job to collect additional information is successful or not.

See Also

- [Collecting Additional Information for Service Now Incidents and Cases Overview](#) on page 334
- [Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident](#) on page 335
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case](#) on page 345
- [Deleting the Settings for Collecting Additional Information for an Incident](#) on page 341

Modifying the Settings for Collecting Additional Information for an Incident

If the job to collect additional information is not already executed, you can modify the following attributes in a configuration for collecting additional information about an incident:

- Junos OS commands configured for collecting additional information
- Date and time the commands should be executed
- interval for executing the commands if the commands are configured to be executed repeatedly

To modify the configuration for collecting additional information for an incident:

1. From the Service Now Navigation tree, select **Service Central > Incidents**.

The Incidents page appears.

2. Select the incident for which you want to modify the settings for collecting additional information.

3. Select **Collect Additional Information > Modify** from the Actions list or the right-click menu.

The Modify Collect Additional Information page appears as shown in [Figure 114 on page 340](#).



NOTE: The Modify option is disabled if the job to collect additional information is in progress or already complete.

Figure 114: Modify Collect Additional Information page

Modify Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: show version

☒ **Schedule at a later time**

Start: 05/21/17 6:28 PM IST

☒ **Repeat**

Interval: Minutes Every 2 Minutes

Ends on: ☒ Never ☐ 05/21/17 6:28 PM IST

Submit **Cancel**

4. (Optional) Modify the commands in the **CLI Commands** text box.
5. (Optional) Modify the schedule for executing the commands under the **Schedule at a later time** section.
6. (Optional) Modify the frequency at which the commands should be executed under the **Repeat** section.
7. Click **Submit**.
 The job to collect information is rescheduled and the job ID is displayed.
8. (Optional) Click the job ID to view the job details.
 The Job Details page displays the progress of the job.

- See Also**
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)
 - [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)

- [Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident on page 335](#)
- [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 348](#)

Deleting the Settings for Collecting Additional Information for an Incident

You can delete a non-recurring configuration for collecting additional information that is scheduled to be executed later by deleting the job from the Jobs workspace of the Service Now navigation tree.

A recurring configuration can be deleted by modifying the configuration. When you modify a recurring configuration, the old configuration is deleted and a new configuration is created with the modifications. You can modify a recurring configuration even if it is already executed one or more number of times. If you want to delete the recurring configuration entirely, then the configuration has to be deleted from the Jobs workspace.

To delete a configuration for collecting additional information from the Jobs workspace:

1. On the Service Now navigation tree, click **Jobs > Job Management**.

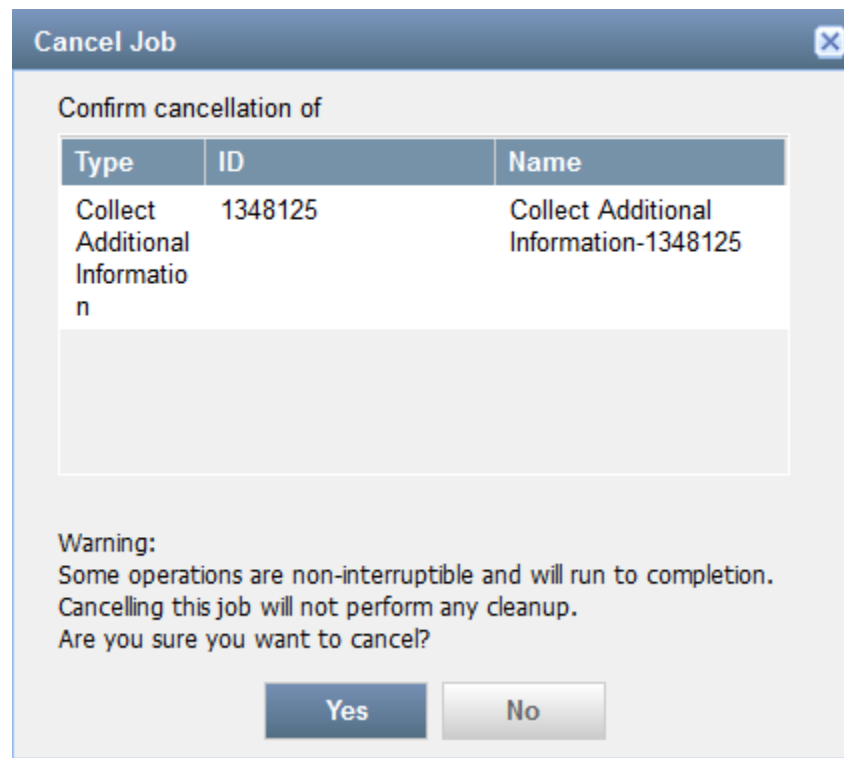
The Job Management page appears.

2. Select the Collect Additional Command job to be deleted.

3. Select **Cancel Job** from the Actions list or the right-click menu.

A confirmation message appears as shown in [Figure 115 on page 342](#).

Figure 115: Cancel Job Dialog Box



4. Click **Yes**.

The job is canceled and the **State** of the job is changed to **Cancelled** from **Scheduled**.

- See Also**
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)
 - [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
 - [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 351](#)

Downloading the Additional Information Collected About an Incident

You can download the additional information collected about an incident from the Collect Additional Information Attachment Details tab of the Incident Detail page. The Collect Additional Information Attachment Details tab of the Incident Detail page provides the following information and the **Download all additional information attachments** link to download the attachments:

- Name of the file containing the additional information
- Size of the file (in bytes)

- User who configured the Junos OS commands to be executed for collecting additional information
- Status of reading the additional information collected on a device
- Status of uploading the additional information to JSS or Service Now partner



NOTE: Incidents for which a technical support case does not exist, the upload status is displayed as **Not Uploaded**.

- Remarks, if any, about the additional information collected for the incident

To download the additional information collected for an incident:

1. On the Service Now navigation tree, select **Service Central > Incidents**.

The Incidents page appears.

2. Double-click the incident for which you want to download additional information collected.

The Incident Detail page appears as shown in [Figure 116 on page 343](#).

Figure 116: Collect Additional Information Attachment Details Tab on the Incident Details Page

Incident Detail					
Incident Details	Case Details	Core File Details	Attachment Details	Log File Details	Collect Additional Information Attachment Details
Download all additional information attachments					
File Name	File Size (in bytes)	Created By	Read Status	Upload Status	Remarks
additional_cli_information_sn-space-ex4550-sys_20170518-113839193.txt	491	super	Success	Success	
additional_cli_information_sn-space-ex4550-sys_20170518-114444902.txt	491	super	Success	Success	
OK					

3. Click the **Collect Additional Information Attachment Details** tab and then click the **Download all additional information attachments** link.

Service Now presents the attachments containing outputs of the additional commands in the *.zip format for download.

4. Download the attachment and save it on your local system.

- See Also**
- [Downloading the Additional Information Collected for a Technical Support Case on page 350](#)
 - [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
 - [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)

Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case

You can view the Junos OS commands configured for collecting additional information for a technical support case on the Collect Additional Information Jobs Results Summary page. The Collect Additional Information Jobs Results Summary page displays the following information:

- Commands executed to collect additional information
- Name of the text file in which the command outputs are collected
- Status of executing the command to collect information
- Date and time the information was collected or is scheduled to be collected
- Job ID for executing the command
- User who configured the command
- Whether or not commands should be executed recurrently
- Remarks, if any

[Figure 117 on page 344](#) shows the Collect Additional Information Jobs Results Summary page.

Figure 117: Collect Additional Information Jobs Results Summary Page

Collect Additional Information Jobs Result Summary							
Back							
Commands	File Name	Job Status	Scheduled Time	Job Id	Owner	Recurrence	Remarks
<input type="checkbox"/> show version	---	Scheduled	May 21, 2017 6:20:41 PM IST	1348115	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550-sys_20170521-124843926.txt	Success	May 21, 2017 6:18:41 PM IST	1348113	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550-sys_20170521-124643891.txt	Success	May 21, 2017 6:16:41 PM IST	1348111	super	Every 2 minutes First Occurrence: 2017-05-21 12:46:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550-sys_20170521-124444786.txt	Success	May 21, 2017 6:14:41 PM IST	1348109	super	Every 2 minutes First Occurrence: 2017-05-21 12:44:41.434	

To view the Junos OS commands configured for collecting additional information:

1. From the Service Now Navigation tree, select **Service Central > View Tech Support Cases**.

The View Tech Support Cases page appears.

2. Select the incident for which you want to view the commands that are configured for collecting additional information.
3. Select **Collect Additional Information > View** from the Actions list or the right-click menu.

The Collect Additional Information Jobs Results Summary page appears. The commands column lists the commands executed for collecting additional information and the Status column indicates whether the commands were executed successfully or not.

- See Also**
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)
 - [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
 - [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 348](#)
 - [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 351](#)
 - [Downloading the Additional Information Collected for a Technical Support Case on page 350](#)

Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case

You can configure Junos OS commands to collect additional information for a technical support case on the View Tech Support Cases page. When you configure additional information to be collected, the commands you configured are executed on the device and the output collected in a *.txt file and uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode).



NOTE:

- A Service Now partner cannot execute Junos OS commands to collect additional information for end-customer support cases. An end customer has to configure the commands for collecting additional information and upload the additional information to the Service Now partner. The Service Now partner, if required, uploads the additional information to JSS.
 - You cannot collect additional information for cases that are closed and cases related to BIOS incidents.
 - For cases associated with a specific siteID (for example, OSSJ cases or cases created by using Case Manager) that are not generated by incidents submitted by Service Now, the option to collect additional information is disabled on the Tech Support Cases page. However, for incidents that are associated with such cases, the option to collect additional information is enabled on the Incidents page.
 - The Junos OS commands configured for collecting additional information are executed on all devices that have incidents related to the technical support case.
-

To collect additional information about a technical support case by executing Junos OS commands:

1. From the Service Now Navigation tree, select **Service Central > View Tech Support Cases**.

The View Tech Support Cases page appears.

2. Select the case for which you want to collect additional information.
3. Select **Collect Additional Information > Create** from the Actions list or the right-click menu.

The Collect Additional Information page appears as shown in [Figure 118 on page 347](#).

Figure 118: Collect Additional Information Page

Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: Multiple commands should be entered as , or ; or new line character.

☒ **Schedule at a later time**
 Start: 05/21/17 6:25 PM IST

☒ **Repeat**
 Interval: Weekly Every 1 Weeks
☒ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

Ends on: ☒ Never
☐ 05/21/17 6:25 PM IST

Submit **Cancel**

- In the CLI Commands text box, enter the commands that you want to execute to collect additional information.



NOTE: Service Now does not validate the commands that you enter to collect additional information. To add multiple commands, use comma (,) or semi-colon (;) or the new line character (press Enter on keyboard) consistently as the delimiter.

- (Optional) Select the **Schedule at a later time** check box and select the date and time the commands should be executed.



NOTE: Service Now executes the commands are executed immediately after you click Submit if you do not schedule a date and time for the commands to be executed.

- (Optional) Select the **Repeat** check box and select the time interval and the frequency of executing the commands.

The intervals can be in minutes, hours, daily, weekly, monthly, or yearly to collect additional information. By default, an interval of once a week is selected.

7. (Optional) To define an end time for collecting information for the incident, do one of the following:

- Click **Never** to continue collecting information by executing the commands at the defined interval till the incident is closed. This option is selected by default.
- Select the date and time when the commands should stop executing.

8. Click **Submit** to save the configuration or **Cancel** to cancel the configuration.

Service Now executes the job to collect additional information immediately if the job is not scheduled for a later time.

See [“Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case” on page 344](#) to check whether the job to collect additional information is successful or not.

- See Also**
- [Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case on page 344](#)
 - [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 336](#)
 - [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 348](#)
 - [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 351](#)
 - [Downloading the Additional Information Collected for a Technical Support Case on page 350](#)
 - [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)

Modifying the Configuration for Collecting Additional Information for a Technical Support Case

If the job to collect additional information is not already executed, you can modify the following attributes in a configuration for collecting additional information for a technical support case:

- Junos OS commands configured for execution to collect additional information
- Date and time the commands should be executed
- Interval for executing the commands if the commands are configured to be executed repeatedly

To modify the configuration for collecting additional information for a technical support case:

1. From the Service Now Navigation tree, select **Service Central > View Tech Support Case**.

The View Tech Support Cases page appears.

2. Select the case for which you want to modify configured commands.
3. Select **Collect Additional Information > Modify** from the Actions list or the right-click menu.

The Modify Collect Additional Information page appears as shown in [Figure 119 on page 349](#).



NOTE: The Modify option is disabled if the job to collect additional information is in progress or complete.

Figure 119: Modify Collect Additional Information Page

Modify Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: show version

☒ **Schedule at a later time**

Start: 05/21/17 6:28 PM IST

☒ **Repeat**

Interval: Minutes Every 2 Minutes

Ends on: ☒ Never ☐ 05/21/17 6:28 PM IST

Submit **Cancel**

4. (Optional) Modify the commands in the **CLI Commands** text box.

5. (Optional) Modify the schedule for executing the commands under the **Schedule at a later time** section.
6. (Optional) Modify the interval at which the commands should be executed under the **Repeat** section.
7. Click **Submit**.
Service Now reschedules the job to collect additional information and displays the job ID.
8. (Optional) Click the job ID to view the job details.
The Job Details page displays the progress of the job.

- See Also**
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 345](#)
 - [Modifying the Settings for Collecting Additional Information for an Incident on page 339](#)
 - [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 351](#)
 - [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)

Downloading the Additional Information Collected for a Technical Support Case

You can download the additional information collected for a technical support case from the Collect Additional Information Attachment Details tab of the Tech Support Case Summary page. The Collect Additional Information Attachment Details tab of the Tech Support Case Summary tab provides the following information and the **Download all additional information attachments** link to download the attachments:

- Name of the file containing the additional information
- Size of the file (in bytes)
- User who configured the commands to be executed for collecting additional information
- Status of reading the additional information collected on a device
- Status of uploading the additional information to JSS or Service Now partner
- Remarks, if any, for the additional information collected

To download the additional information collected for a technical support case:

1. On the Service Now navigation tree, select **Service Central > View Tech Support Case**.
The View Tech Support Cases page appears.
2. Double-click the case for which you want to download additional information collected.

The Tech Support Case Summary page appears.

3. Click the **Collect Additional Information Attachment Details** tab and then click the **Download all additional command attachments** link.

Service Now generates a compressed file, in *.zip format, that contains outputs of the additional commands.

4. Download the attachment and save it on your local system.

- See Also**
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 345](#)
 - [Downloading the Additional Information Collected About an Incident on page 342](#)
 - [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)

Deleting the Configuration for Collecting Additional Information for a Technical Support Case

You can delete a non-recurring configuration for collecting additional information that is scheduled to be executed later by deleting the job from the Jobs workspace of the Service Now navigation tree.

A recurring configuration can be deleted by modifying the configuration. When you modify a recurring configuration, the old configuration is deleted and a new configuration is created with the modifications. You can modify a recurring configuration even if it is already executed one or more number of times. You can delete the recurring configuration from the Jobs workspace.

To delete a configuration for collecting additional information from the Jobs workspace:

1. On the Service Now navigation tree, click **Jobs > Job Management**.

The Job Management page appears.

2. Select the Collect Additional Information job to be deleted and click **Cancel Job** from the Actions list or the right-click menu.

A confirmation message appears as shown in [Figure 120 on page 352](#).

Figure 120: Cancel Job Dialog Box



3. Click **Yes**.

Service Now cancels the job and changes the **State** of the job to **Cancelled** from **Scheduled**.

- See Also**
- [Deleting the Settings for Collecting Additional Information for an Incident on page 341](#)
 - [Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case on page 344](#)
 - [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 345](#)
 - [Collecting Additional Information for Service Now Incidents and Cases Overview on page 334](#)

Information

- [Service Now Messages Overview on page 353](#)
- [Assigning Ownership to Messages on page 353](#)
- [Flagging a Message to Users on page 354](#)
- [Deleting a Message on page 355](#)
- [Assigning a Message to an End Customer on page 355](#)

- [Service Now Device Snapshots Overview on page 357](#)
- [Exporting Device Snapshots to HTML on page 358](#)
- [Generating an On-Demand Device Snapshot on page 359](#)
- [Deleting Device Snapshots on page 361](#)
- [Viewing Details of a Device Snapshot on page 362](#)

Service Now Messages Overview

Service Now polls Juniper Support Systems (JSS) regularly for information messages such as notifications for JSS downtime and availability of new Service Now, Service Insight, or AI-Scripts releases for download. These information messages are displayed on the Service Now Messages page (**Service Central > Information > Messages**). Service Now allows you to assign the information message to a user for ownership and flag it to one or more users. This ensures that users are kept informed of changes made to information messages.

Associated Actions

You can perform the following actions related to messages:

- View list of information messages received from JSS
- Assign an owner to an information message; see [“Assigning Ownership to Messages” on page 353](#) for details.
- Assign messages to connected members.
- Flag an information message to users; see [“Flagging a Message to Users” on page 354](#) for details.
- Delete information messages; see [“Deleting a Message” on page 355](#) for details.
- Scan for devices impacted by the message; see *Scanning a Message for Impact* for details.

- See Also**
- [Service Now Device Snapshots Overview on page 357](#)
 - [Service Now Organizations Overview on page 99](#)

Assigning Ownership to Messages

Junos Space Service Now provides the Assign Ownership option on the Actions list to assign a user to take up ownership of the 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.

- See Also**
- [Flagging a Message to Users on page 354](#)
 - [Scanning a Message for Impact](#)
 - [Deleting a Message on page 355](#)
 - [Assigning a Message to an End Customer on page 355](#)
 - [Viewing Messages Assigned to an End Customer on page 109](#)
 - [Service Now Messages Overview on page 353](#)
 - [Service Now Device Snapshots Overview on page 357](#)

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 Junos Space 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**.

Service Now notifies the specified users about the selected information message.

- See Also**
- [Service Now Device Snapshots Overview on page 357](#)
 - [Assigning Ownership to Messages on page 353](#)

- [Scanning a Message for Impact](#)
- [Deleting a Message on page 355](#)
- [Assigning a Message to an End Customer on page 355](#)
- [Viewing Messages Assigned to an End Customer on page 109](#)
- [Service Now Messages Overview on page 353](#)

Deleting a Message

Junos Space Service Now provides the Delete option on the Actions list to delete information messages from the Service Now database.

To delete an information message:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.
The Messages page appears.
2. Select one or more 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.

Service Now deletes the selected information messages from the Service Now database and removes them from the Messages page.

- See Also**
- [Service Now Device Snapshots Overview on page 357](#)
 - [Assigning Ownership to Messages on page 353](#)
 - [Flagging a Message to Users on page 354](#)
 - [Scanning a Message for Impact](#)
 - [Assigning a Message to an End Customer on page 355](#)
 - [Viewing Messages Assigned to an End Customer on page 109](#)
 - [Service Now Messages Overview on page 353](#)

Assigning a Message to an End Customer

Junos Space Service Now polls Juniper Support Systems (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 Direct, 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 121 on page 356](#), 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 121: Choose Connected Members Dialog Box

Connected Members Assigned to the selected Information Update		
Site Name	Status	Sent
EndCustomer1	Staged for Connected Member	

Connected Members Unassigned to the selected Information Update
Site Name

Warning: Messages once assigned to a Connected Member cannot be deleted.

Submit **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 109](#).

See Also • [Adding an End Customer to Service Now Configured in Partner Proxy Mode on page 104](#)

- [Service Now Device Snapshots Overview on page 357](#)
- [Assigning Ownership to Messages on page 353](#)
- [Flagging a Message to Users on page 354](#)
- [Scanning a Message for Impact](#)
- [Deleting a Message on page 355](#)
- [Viewing Messages Assigned to an End Customer on page 109](#)
- [Service Now Messages Overview on page 353](#)

Service Now Device Snapshots Overview

Junos Space Service Now periodically collects device snapshots [also known as informational Juniper Message Bundles (iJMBs)] that contain configuration and trend information of devices. Service Now displays the iJMBs on the Device Snapshot page (**Service Central > Information > Device Snapshots**). By default, Service Now sends the iJMBs to Juniper Support Systems (JSS) or Service Now Partner for processing. 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 if the device is susceptible to known issues.

If AI-Scripts is installed on a device, device snapshots are generated once every 7 days. Service Now collects the device snapshot and shares it with JSS or Service Now partner for analysis. Before sharing the device snapshots, Service Now filters the configuration information in the device snapshot based on the **JMB Filter Level** set for the organization to which the devices belongs. For information about JMB filter levels, see [“Adding an Organization to Service Now” on page 102](#)

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.

When Service Now detects that a device has not generated iJMB for more than seven days, it generates on-demand device snapshots by using the **directive.rc** file and shares it with JSS or Service Now partner. Service Now also detects devices that have stopped sending device snapshots for more than two weeks and displays them graphically on the Administration page. To view details of such devices, you can click the Devices Not Sending Snapshots bar of the Devices Not Sending Device Snapshots graph. Service Now opens the Service Now Devices page where you can view their details and export the device details to an Excel file.

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; SNMP traps are not sent.

Associated Actions

You can perform the following actions related to device snapshots:

- Export device snapshots in HTML format; see [“Exporting Device Snapshots to HTML” on page 358](#) for details.
- Delete device snapshots; see [“Deleting Device Snapshots” on page 361](#) for details.
- View device snapshots; see [“Viewing Details of a Device Snapshot” on page 362](#) for details.

- See Also**
- [Service Now Messages Overview on page 353](#)
 - [Monitoring Device Snapshots](#)
 - [Adding an Organization to Service Now on page 102](#)
 - [AI-Scripts Overview on page 35](#)

Exporting Device Snapshots to HTML

Junos Space Service Now provides the Export iJMB to HTML option in the Actions list of the Device Snapshots page to export device snapshots collected by Service Now in HTML format. Service Now exports iJMBs as a zipped folder. The view of the exported JMB file is the same as that of the Juniper Message Bundle (JMB) page in Service Now.

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 device snapshot that you want to export, and select **Export iJMB 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.

- See Also**
- [Service Now Device Snapshots Overview on page 357](#)
 - [Deleting Device Snapshots on page 361](#)
 - [Viewing Details of a Device Snapshot on page 362](#)
 - [Service Now Messages Overview on page 353](#)

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).



NOTE: You cannot create an on-demand device snapshot for a device if the device is not associated with a device group.

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 one or more devices for which you want to generate an on-demand device snapshot.

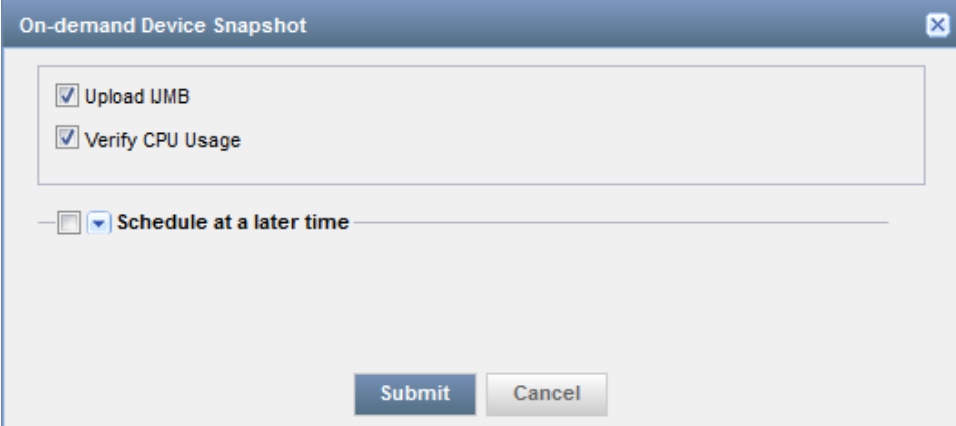


NOTE: You can create on-demand incidents for up to five devices simultaneously.

3. From the Actions list, select **Device Operations > Create On-Demand Device Snapshots**. Alternatively, right-click the selected devices and select **Device Operations > Create On-Demand Device Snapshots**.

The On-demand Incident dialog box appears as shown in [Figure 122 on page 360](#).

Figure 122: On-demand Incident Dialog Box



The dialog box is titled "On-demand Device Snapshot" and contains the following options:

- ☒ Upload IJMB
- ☒ Verify CPU Usage
- ☐ Schedule at a later time

At the bottom right, there are two buttons: "Submit" and "Cancel".

- (Optional) Clear the **Upload iJMB** check box to prevent Service Now from automatically uploading the to Juniper Support Systems (JSS) or Service Now partner.

By default, the check box is selected and iJMBs are automatically uploaded to JSS or Service Now partner..

- (Optional) Clear the **Verify CPU Usage** check box to avoid Service Now from 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 32 on page 360](#), 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 32: 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

- (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 device snapshot be generated.

- Click **Submit**.

Service Now creates a job for generating the device snapshot and displays the job ID as a link in the Job information dialog box.

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.
- Service Now lists the device snapshot on the Device Snapshots page.

- See Also**
- [Service Now Devices Overview on page 117](#)
 - [Assigning an Auto Submit Policy to a Device on page 148](#)
 - [Service Now Incidents Overview on page 302](#)

Deleting Device Snapshots

Junos Space 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 configurable on the Device Snapshot Purge Time (in days) parameter on the Global Settings page. For information about configuring a purge time for device snapshots, see [“Configuring Global Settings” on page 191](#).

Service Now provides the Delete option on the Actions list on the Device Snapshots page to delete device snapshots 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 device snapshot 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.

Service Now deletes the device snapshot from the Service Now database and removes them from the Device Snapshots page.

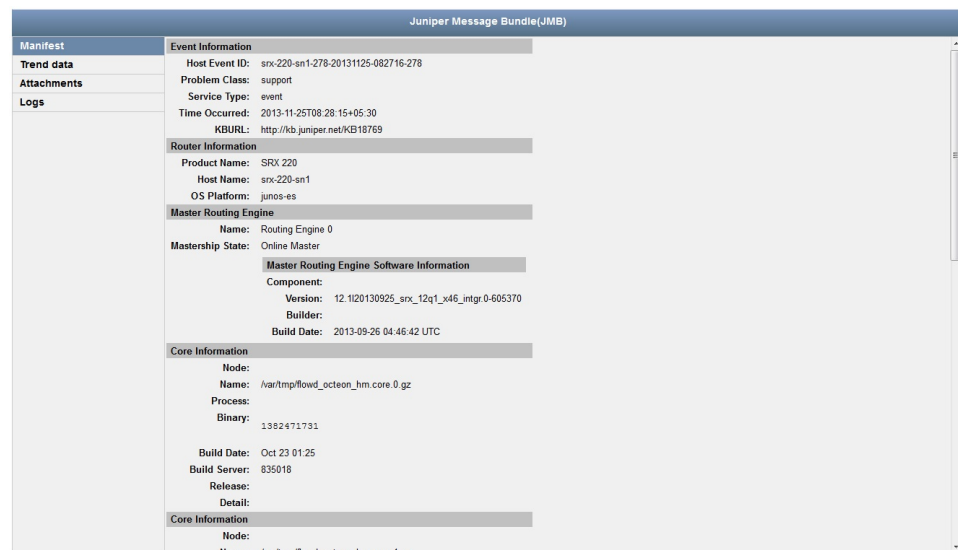
- See Also**
- [Service Now Device Snapshots Overview on page 357](#)
 - [Exporting Device Snapshots to HTML on page 358](#)
 - [Viewing Details of a Device Snapshot on page 362](#)
 - [Service Now Messages Overview on page 353](#)
 - [Junos Space Service Now Global Settings Overview](#)

Viewing Details of a Device Snapshot

When Junos Space 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 123 on page 362](#). You can click the links in the Attachments and Logs sections to view or download attachments and system log files.

Figure 123: Juniper Message Bundle



To view details of a JMB:

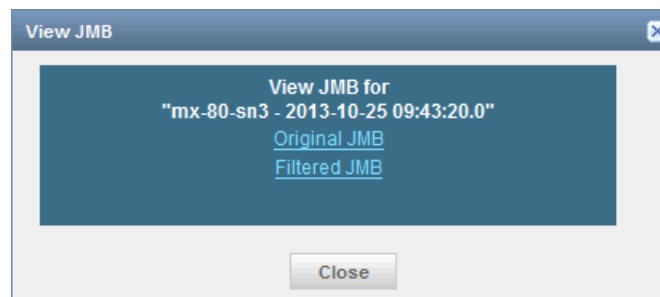
1. From the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.

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 list, 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 124 on page 363](#). The information in the filtered JMB is displayed based on the JMB filter level set for the organization associated with the device for which the JMB is generated.

Figure 124: 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 defined by the JMB filter level set for the organization associated with the device for which the JMB is generated.

- See Also**
- [Service Now Device Snapshots Overview on page 357](#)
 - [Exporting Device Snapshots to HTML on page 358](#)
 - [Deleting Device Snapshots on page 361](#)
 - [Service Now Messages Overview on page 353](#)

Device Analysis

- [Viewing BIOS Validations on page 363](#)
- [Exporting BIOS Validation Results on page 366](#)
- [Deleting BIOS Validation Incidents on page 367](#)
- [Viewing Product Health Data Files Collected from a Device on page 368](#)
- [Exporting Product Health Data Information to an Excel File on page 371](#)
- [Deleting Product Health Data Files Collected from a Device on page 376](#)

Viewing BIOS Validations

On its dashboard, the Device Analysis task displays the status and results of the BIOS validations and product health data 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 one 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 33 on page 364 lists the information Service Now provides about BIOS validation incidents.

Table 33: BIOS Validations Field Descriptions

Field Name	Description
Incident Details	
Device	Device for which BIOS validation was performed
IP Address	IP address of the device
Device Serial Number	Serial Number of the device
Product	Product family to which the device belongs
Platform	Routing software used in the device; for example, Junos, Junos-es
Release	Release number of the routing software
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
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. <p>NOTE: This status is not applicable when Service Now is operating in 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 status is not applicable when Service Now is operating in 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—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.

Table 33: BIOS Validations Field Descriptions (continued)

Field Name	Description
Problem Identifier	ID of the BIOS incident
Event Type	Event type of the incident The value is usually BIOS Collection.
Defect Type	Defect type of the incident The value is usually BIOS Collection.
Job Id	ID of the job used to created the BIOS validation incident
Filter Name	Incident filter, if any, used to create the BIOS validation incident
KB Article	Link to the Knowledge Base (KB) article to understand BIOS integrity validation events
Attachment Details	
Attachment	Name of the attachment file You cannot view the contents of the attachment file.
Attachment Size (in bytse)	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, if any, about issues while collecting or uploading the attachment.
Log File Details	
Log File	The system log file collected as part of BIOS validation You cannot view the contents of the system log files.
Log File Size (in bytes)	Size of log files in bytes.
Read Status	Status of reading the log files
Remarks	Remarks, if any, about the issues while collecting or uploading system log files.

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

- Delete BIOS validations; see [“Deleting BIOS Validation Incidents” on page 367](#)
- Export information about BIOS validation results to Excel, see [“Exporting BIOS Validation Results” on page 366](#)

- See Also**
- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 162](#)
 - [Service Now Product Health Data Collection Overview on page 254](#)

Exporting BIOS Validation Results

You can export the details of BIOS validation incidents of managed devices to an Excel file for reference. [Table 34 on page 366](#) lists the BIOS validation information exported to an Excel file.

Table 34: 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
BIOS Result	Status of BIOS validation: <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 Systems (JSS) or Service Now partner for validation. • Submitted—Service Now has submitted the BIOS data for validation. • Submission Failed—Service Now is unable to submit the BIOS data. for validation • Validation Success—Validation of BIOS data 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 or Service Now
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 details:

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 list, 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.

- See Also**
- [Service Now BIOS Validation Overview on page 160](#)
 - [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 162](#)
 - [Viewing BIOS Validations on page 363](#)
 - [Deleting BIOS Validation Incidents on page 367](#)

Deleting BIOS Validation Incidents

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 incident if the status of BIOS validation 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 incidents to be deleted.
3. From the Actions list, 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 incident or **Cancel** to cancel the deletion.

If you click Delete, Service Now deletes the BIOS validation incidents and removes them from the BIOS Validations page.

- See Also**
- [Service Now BIOS Validation Overview on page 160](#)
 - [Viewing BIOS Validations on page 363](#)
 - [Configuring BIOS Validation for Verifying BIOS Integrity of a Device on page 162](#)
 - [Exporting BIOS Validation Results on page 366](#)

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 Systems (JSS) or Service Now partner 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 125 on page 368](#). 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 125: 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

Table 35: 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

Table 35: Fields on the View All Product Health Data Files Page (continued)

Field Name	Description
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.
Upload Status	<p>Status of uploading PHD files to JSS:</p> <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 or Service Now partner

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 126 on page 370](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 126: View All Devices of this PHDC Page

Applications Administration > Product Health Data Collection > View all Devices of this PHDC						
Back						
Device	Serial Number	Product	Start Date	Status	Total Files Available	
snv-220-sn1	AG5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0	
snv-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.

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

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

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

- See Also**
- [Service Now Product Health Data Collection Overview on page 254](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)
 - [Exporting Product Health Data Information to an Excel File on page 276](#)
 - [Deleting Product Health Data Files Collected from a Device on page 281](#)
 - [Deleting a Product Health Data Collection Configuration from Service Now on page 283](#)

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 was created.

[Figure 127 on page 371](#) shows a sample of the information about devices exported to Excel.

Figure 127: 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 *yyyy-mm-dd* and *hhmmss* are the date and time the Excel file was created.

[Figure 128 on page 372](#) shows a sample of the information about PHD files exported to Excel.

Figure 128: 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 372](#)
- [Exporting Data about PHD Files Collected from a Device on page 374](#)

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 129 on page 373](#). The View all Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 129: View all Devices of this PHDC

Device	Serial Number	Product	Start Date	Status	Total Files Available
snv-220-en1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snv-650-en2	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 130 on page 375](#).

Figure 130: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_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 131 on page 375](#).

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

Figure 131: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
sr1-220-sr1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
sr1-650-sr2	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**.

Service Now displays the Export All Product Health Data Information dialog box.

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**.

Service Now displays the Export Selected Product Health Data Information dialog box. 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.

- See Also**
- [Service Now Product Health Data Collection Overview on page 254](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)

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 Systems (JSS) or Service Now partner for assessing the health of the device. If configured to be deleted, the PHD files are deleted immediately after they are uploaded to JSS or Service Now partner. Otherwise, the PHD files are deleted from the Service Now database four days after they are generated.

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 132 on page 377](#).

Figure 132: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

- To delete the PHD files from the Product Health Data Collection task of the Administration workspace:

- 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 133 on page 377](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 133: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
srn-220-sr1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
srn-650-sr2	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 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.

- See Also**
- [Service Now Product Health Data Collection Overview on page 254](#)
 - [Product Health Data Collection Configuration Overview on page 259](#)
 - [Viewing Product Health Data Files Collected from a Device on page 256](#)
 - [Exporting Product Health Data Information to an Excel File on page 276](#)

JMB Errors

- [JMBs with Errors on page 378](#)

JMBs with Errors

Junos Space 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 erroneous JMBs 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 379](#)
- [Deleting JMBs with Errors on page 380](#)

Downloading JMBs with Errors

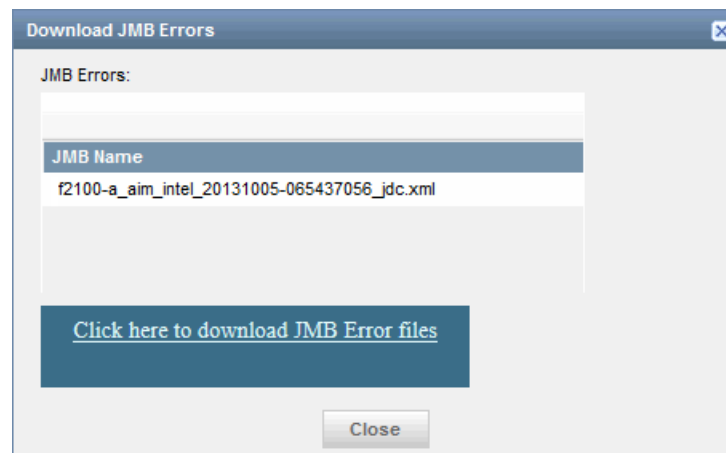
When you download a JMB, it is saved as a zip file. You can download up to five erroneous JMBs at a time.

To download erroneous JMBs:

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 (upto five JMBs) that you want to download.
3. From the Actions list, 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 134 on page 379](#).

Figure 134: 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.

See Also

Deleting JMBs with Errors

You can delete multiple erroneous JMBs 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 list, select **Delete**. Alternatively, right-click and select **Delete**.

Service Now displays the Delete Error JMB dialog box and 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.

- See Also**
- [Service Central Overview on page 299](#)
 - [Service Now Messages Overview on page 353](#)

Suppressed Events

- [Service Now Suppressed Events Overview on page 380](#)
- [Deleting JMBs for Suppressed Events on page 381](#)
- [Viewing Details of JMBs for Suppressed Events on page 382](#)
- [Creating Incidents for Suppressed Juniper Message Bundles on page 383](#)

Service Now Suppressed Events Overview

Suppressed Events are events for which Junos Space Service Now does not create incidents as the JMBs for the events are filtered by incident filters. Starting in Junos Space Service Now Release 17.1R1, you can view events that were suppressed on the Suppressed Events page (**Service Central > Suppressed Events**) and, if required, create incidents for the suppressed events.

[Figure 135 on page 381](#) shows the Suppressed Events page .

Figure 135: Suppressed Events Page

Organization	Device Group	Received Time	Device	Event Name	JMB Name	Problem Identifier
Prod_Org	Default for TestORG	May 17, 2017 6:58:46 PM IST	sn-space-ex4550-sys	CHASSISD_CFE_POWER_FAIL_URE	sn-space-ex4550-sys_20170516_142502_411_jmb	sn-space-ex4550-sys-411-20170516-142311-4

Associated Actions

You can perform the following actions related to suppressed events:

- Delete JMBs for suppressed events; see [“Deleting JMBs for Suppressed Events” on page 381](#) for details.
- View JMBs for suppressed events; see [“Viewing Details of JMBs for Suppressed Events” on page 382](#) for details.
- Create incident for the suppressed events; see [“Creating Incidents for Suppressed Juniper Message Bundles” on page 383](#) for details.

- See Also**
- [Service Now Incident Filters Overview on page 207](#)
 - [Service Now Auto Submit Filters Overview on page 222](#)

Deleting JMBs for Suppressed Events

Junos Space Service Now provides the Delete option in the Actions list of the Suppressed Event page to delete JMBs for which incidents are not created.

1. In the Service Now navigation tree, click **Service Central > Suppressed Events**.

The Suppressed Events page appears.

2. Select one or more JMBs that you want to delete and select **Delete** from the Actions list or the right-click menu.

The Delete Suppressed Events dialog box appears as shown in [Figure 136 on page 382](#).

Figure 136: Delete Suppressed Events Dialog Box

3. Click **Delete**.

The selected JMBs are deleted and are not listed on the Suppressed Events page.

- See Also**
- [Viewing Details of JMBs for Suppressed Events on page 382](#)
 - [Service Now Suppressed Events Overview on page 380](#)
 - [Creating Incidents for Suppressed Juniper Message Bundles on page 383](#)

Viewing Details of JMBs for Suppressed Events

You can view the details of the JMBs that were filtered by incident filters defined to not create incidents on the Suppressed Events page. The Suppressed Events page displays the following information about a JMB:

- **Organization**—The organization with which the JMB is associated
- **Device Group**—The device group with which the device from which the JMB was generated is associated
- **Received Time**—The date and time the JMB was received by Service Now
- **Device**—The device from which the JMB was generated
- **Event Name**—The event that triggered the generation of JMB
- **JMB Name**—The name of the JMB
- **Problem Identifier**—The ID of the event that occurred on the device
- **Filter**—The filter used to suppress incident creation for the JMB

- Product—The Juniper Networks product on which the JMB was created
- Priority—Priority of the event

To view details of JMBs for suppressed events:

1. In the Service Now navigation tree, click **Service Central > Suppressed Events**.

The Suppressed Events page appears.

2. Select a JMB for viewing details.

The JMB details page appears. For information about details about JMB, see *Contents of a JMB*.

- See Also**
- [Service Now Suppressed Events Overview on page 380](#)
 - [Creating Incidents for Suppressed Juniper Message Bundles on page 383](#)
 - [Deleting JMBs for Suppressed Events on page 381](#)

Creating Incidents for Suppressed Juniper Message Bundles

You can create incidents for JMBs suppressed by incident filters. This option is helpful when you have exceptions to incident filters that are defined to not create incidents.

To create incidents for suppressed JMBs:

1. In the Service Now navigation tree, click **Service Central > Suppressed Events**.

The Suppressed Events page appears.

2. Select one or more JMBs for which you want to create incidents and select **Create Incident** from the Actions list or the right-click menu.

The Create Incident Suppressed JMBs dialog box appears as shown in [Figure 137 on page 384](#).

Figure 137: Create Incident for Suppressed JMBs Dialog BoxA screenshot of a web-based dialog box titled "Create Incident Suppressed JMBs". The dialog box has a blue header bar with the title and a close button (X) in the top right corner. Below the header, the text "Confirm creation of:" is displayed. Underneath this text is a large, light gray rectangular area. Within this area, there is a blue header bar labeled "JMB Name". Below the "JMB Name" header, the text "sn-space-ex4550-sys_20170516_142502_411_jmb_ais_prob.xml" is displayed. At the bottom of the dialog box, there are two buttons: a blue "Create" button and a gray "Cancel" button.

3. Click **Create**.

The Create Incident for Suppressed JMBs dialog box appears.

4. Click **Create**.

Service Now creates a new incident and lists it on the Incidents page. The JMB is removed from the Suppressed Events page.

- See Also**
- [Service Now Suppressed Events Overview on page 380](#)
 - [Viewing Details of JMBs for Suppressed Events on page 382](#)
 - [Deleting JMBs for Suppressed Events on page 381](#)

Notifications

- [Service Now Notification Policies Overview on page 384](#)
- [Creating and Editing a Notification Policy on page 386](#)
- [Enabling or Disabling a Notification Policy on page 395](#)
- [Deleting a Notification Policy on page 395](#)

Service Now Notification Policies Overview

Junos Space 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, such as new incident created, a case created for

the incident, or a device snapshot received, for which you want Service Now to send a notification.

You can view notification policies configured in Service Now on the Notifications page (**Service Central > Notifications**).

You must specify the following parameters when you create a notification policy:

- **Trigger**—The event (for example, device snapshot received for a device) that causes Service Now to send notification
- **Filters**—Filters for the events that cause Service Now to send a notification
- **Actions**—List of user e-mail IDs and SNMP trap destinations to which the notifications must be sent when the event occurs..

Table 36 on page 385 lists the triggers and filters that can be configured on Service Now.

Table 36: Notification Triggers and Trigger Filters

Trigger	Description	Filters
New Incident Detected	Trigger to send a notification when a new incident is received from a Service Now Device. This is the only option available when Service Now is in offline mode.	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 Systems (JSS) or Service Now partner	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
Service Contract Expiring	Trigger to send a notification when the technical support contract license is nearing expiry for one or more devices The notification is sent sixty days before expiry of the service contract and lists devices for which the technical support contract is nearing expiry	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

Table 36: Notification Triggers and Trigger Filters (continued)

Trigger	Description	Filters
Ship-to Address Missing For Device	Trigger to send a notification when an RMA incident is submitted to JSS or Service Now partner 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 from a device 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

Associated Actions

You can perform the following actions related to notifications:

- Edit filters and actions configured for a trigger; see [“Creating and Editing a Notification Policy” on page 386](#) for details.
- Enable or disable a notification policy; see [“Enabling or Disabling a Notification Policy” on page 395](#) for details.
- Delete a notification policy; see [“Deleting a Notification Policy” on page 395](#) for details.

- See Also**
- [Service Now Incidents Overview on page 302](#)
 - [Service Now Technical Support Cases and End Customer Support Cases Overview on page 326](#)
 - [Service Now Messages Overview on page 353](#)
 - [Service Now Device Snapshots Overview on page 357](#)
 - [Service Now BIOS Validation Overview on page 160](#)
 - [Service Now Product Health Data Collection Overview on page 254](#)
 - [Service Now E-Mail Templates Overview on page 293](#)

Creating and Editing a Notification Policy

Notification policies specify when you want Junos Space 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 define the trigger events, and the users and the SNMP trap destinations to which you want the notifications should be sent.

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 138 on page 387](#),

Figure 138: Create Notifications Page

2. In the **Name** text field, enter a name for the 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. From the **Trigger** list, select an event in Service Now for which you want to send notifications.

For the list of triggers, see [Table 36 on page 385](#).

4. Expand the Apply Filters section if not already expanded, and enter values for the filter parameters.

The filter parameters displayed depend on the trigger you chose in the Trigger list.

5. Under the Actions section, enter the e-mail IDs of users to whom a notification must be sent for the selected trigger.

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

6. Under the Send SNMP Traps to section, select the destination where SNMP traps must be sent for the selected trigger.

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

8. Click **Add**.

Service Now creates the notification policy and lists it 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 37 on page 389](#).

Table 37: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Remark
Name	Enter a unique name for the policy.	64 characters	–

Table 37: 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 37: 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 37: 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 37: 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 37: 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 37: 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 194 .	–	–

- See Also**
- [Service Now Notification Policies Overview on page 384](#)
 - [Enabling or Disabling a Notification Policy on page 395](#)
 - [Deleting a Notification Policy on page 395](#)

Enabling or Disabling a Notification Policy

Notification policies specify the events for which Junos Space 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.

- See Also**
- [Service Now Notification Policies Overview on page 384](#)
 - [Creating and Editing a Notification Policy on page 386](#)
 - [Deleting a Notification Policy on page 395](#)

Deleting a Notification Policy

A notification policy specifies the events for which Junos Space 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 one or more notification policies 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**.

Service Now deletes the selected notification policies from the Service Now database and from the Notifications page.

- See Also**
- [Service Now Notification Policies Overview on page 384](#)
 - [Creating and Editing a Notification Policy on page 386](#)
 - [Enabling or Disabling a Notification Policy on page 395](#)

PART 3

Junos Space Service Insight

- [Introduction to Service Insight on page 399](#)
- [User Roles on page 407](#)
- [Insight Central on page 409](#)

CHAPTER 8

Introduction to Service Insight

- [Service Insight Overview on page 399](#)

Service Insight Overview

- [Service Insight Overview on page 399](#)
- [Service Insight Domain Overview on page 403](#)

Service Insight Overview

Junos Space Service Insight is an application that helps in accelerating operational analysis and managing the exposure of network devices running Junos OS 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 102](#) section in the *Junos® Space Service Now User Guide*.

Service Insight identifies the devices containing EOL parts and enables you to generate reports that provide detailed information about EOL parts in managed devices. Service Insight provides the following EOL information:

- Number of devices with parts that are EOL
- EOL announcement date
- Number of announced parts that are EOL
- End of software engineering date
- Number of software parts that are at end of engineering
- End of hardware engineering date
- Number of hardware parts that are at end of engineering
- End of Support date
- Number of end of support parts
- Top-level assembly parts
- Circuit assembly parts

- Product serial numbers
- Replacement numbers

Apart from providing EOL information, 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 [“Service Insight Targeted PBNs Overview” on page 430](#).

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 [“Service Insight Notifications Overview” on page 435](#).

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. For information about Service Insight timers, see *Junos Space Service Now and Junos Space Service Insight Timers*.

- [Service Insight Dashboard on page 401](#)
- [Dashboard Gadgets on page 401](#)
- [Service Insight Workspaces on page 403](#)
- [Benefits of Junos Space Service Insight on page 403](#)

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:

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.

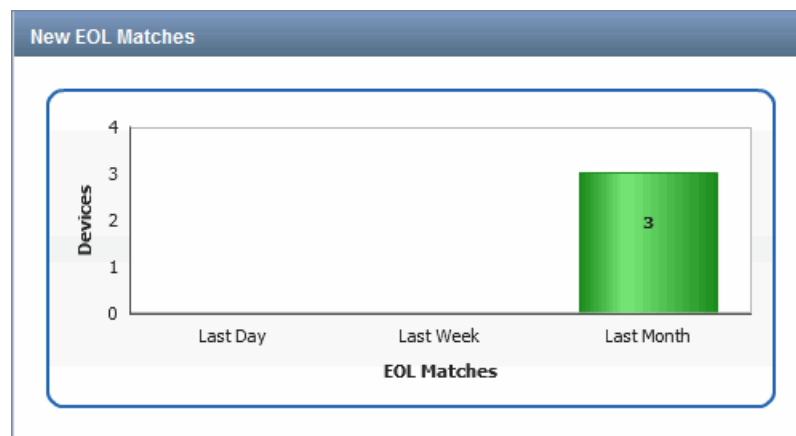
Service Insight displays the following gadgets:

- [New EOL Matches on page 401](#)
- [Recent PBNs on page 401](#)
- [PBN Severity on page 402](#)
- [Service Insight Notices on page 402](#)

New EOL Matches

The **New EOL Matches** gadget graphically displays the number of devices found with EOL parts 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 details of devices with EOL parts.

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 three devices for which EOL notifications were received last month.

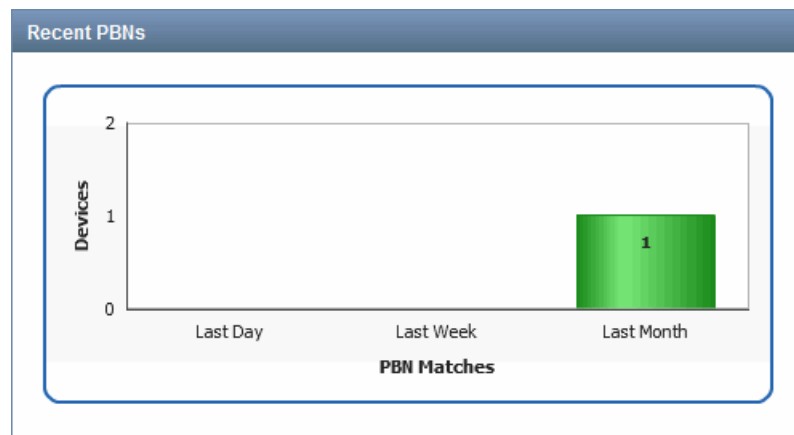


Recent PBNs

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 were received.

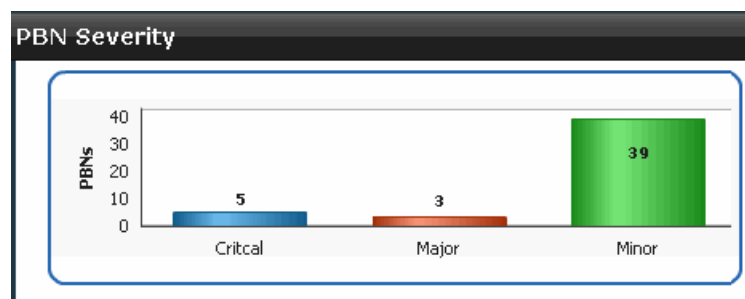
For example, when you click the green bar of the **Recent PBNs** gadget (as shown in the following figure), the **Manage PBNs** page lists only one device for which PBNs were received last month.



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: <https://www.juniper.net/alerts/>
- EOS information: <https://www.juniper.net/support/eol/>

Service Insight Workspaces

- **Insight Central**—Provides gadgets to view new devices with EOL parts and PBNs received recently. It also provides options to generate EOL PBN reports, EOL reports, and lists targeted PBNs. See [“Insight Central Overview” on page 409](#) for details.

For more information about Insight Central workspace, see .

- **Devices**—Same as the Devices workspace in Junos Space Network Management Platform. See *Device Management Overview* for details.
see .
- **Jobs**—Same as the Devices workspace in Junos Space Network Management Platform. See *Jobs Overview* for details.
- **Administration**—This is the same as the Administration workspace in Service Now. See [“Service Now Administration Workspace Overview” on page 97](#) for details.

Benefits of Junos Space Service Insight

- Provides PBNs that identify specific devices in your network that might be susceptible to known issues before the issues impact the devices.
- Helps you plan the hardware and software maintenance of your network by analyzing the impact of a device or device parts at EOL or EOS.
- Works with Service Now to make asset tracking easier by providing asset details (including support contract information) for managed Juniper devices, saving time spent in manual tracking of the assets.

- See Also**
- [Insight Central Overview on page 409](#)
 - [Service Insight Domain Overview on page 403](#)

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 *Domains Overview* in the *Workspaces Feature Guide* available at https://www.juniper.net/documentation/en_US/junos-space18.1/index.html.

When you access Junos Space 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 404](#).

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 38 on page 404](#) lists Service Insight objects and their default domains.

Table 38: 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 list, 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.

5. To verify that the object is assigned to the correct domain, from the **Login as *username*** in list, select the domain to which you assigned the object.

The Service Insight GUI is refreshed.

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

- See Also**
- [Insight Central Overview on page 409](#)
 - [Service Now Administration Workspace Overview on page 97](#)
 - [Domains Overview](#)

User Roles

- [Junos Space Service Insight User Roles on page 407](#)

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 39 on page 407](#) 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 39: 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 39: 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 User Accounts in Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide* available at

https://www.juniper.net/documentation/en_US/release-independent/junos-space/index.html.

Related Documentation

- [User Roles and Permissions Overview](#)
- [Insight Central Overview on page 409](#)
- [Junos Space Service Now User Roles on page 74](#)

CHAPTER 10

Insight Central

- [Insight Central Overview on page 409](#)
- [Exposure Analyzer on page 410](#)
- [Managing EOL Reports on page 419](#)
- [Managing PBN Reports on page 425](#)
- [Managing PBNs on page 429](#)
- [Managing Notifications on page 435](#)

Insight Central Overview

- [Insight Central Overview on page 409](#)

Insight Central Overview

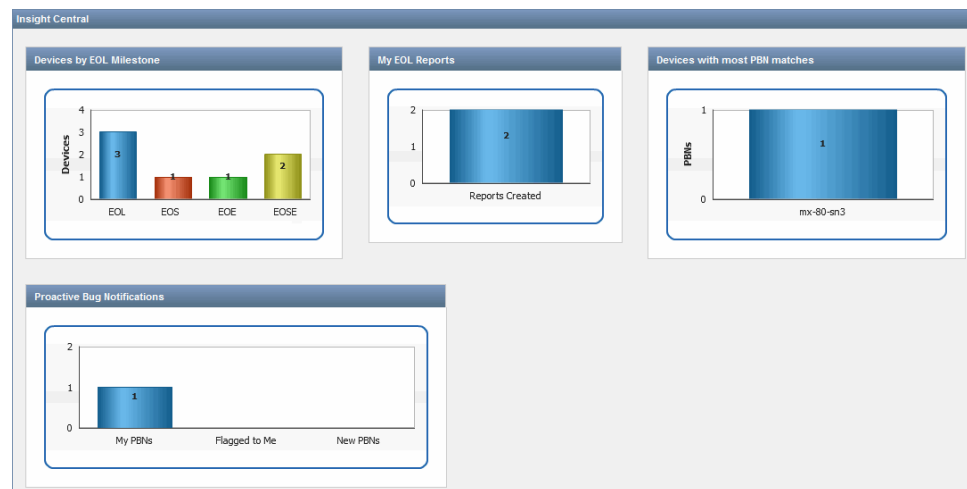
- [Insight Central Overview on page 409](#)

Insight Central Overview

Insight Central is a Service Insight workspace where you can manage End Of Life (EOL) reports and Proactive Bug Notifications (PBNs). The Exposure Analyzer page in 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 SNMP servers to which SNMP traps and the users to whom the notifications must be sent.

To access the Insight Central workspace, you must first enable the Service Insight application. 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 102](#).

The Insight Central landing page (as shown in [Figure 139 on page 410](#)) 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 139: Insight Central Landing Page

- See Also**
- [Service Insight Overview on page 399](#)
 - [Exposure Analyzer Overview on page 410](#)
 - [Service Insight EOL Reports Overview on page 420](#)
 - [Service Insight PBN Reports Overview on page 425](#)
 - [Service Insight Targeted PBNs Overview on page 430](#)
 - [Service Insight Notifications Overview on page 435](#)

Exposure Analyzer

- [Exposure Analyzer on page 410](#)

Exposure Analyzer

- [Exposure Analyzer Overview on page 410](#)
- [Generating EOL Reports on page 413](#)
- [Generating PBN Reports on page 415](#)
- [Viewing PBNs for a Device on page 419](#)

Exposure Analyzer Overview

Junos Space Service Insight lists devices and the number of End of Life (EOL) parts and Proactive Bug Notifications (PBNs) that are applicable for the devices based on EOL reports and PBNs received from Juniper Support Systems (JSS) (see [Figure 140 on page 412](#)). 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 40 on page 412](#) describes these icons. [Table 41 on page 412](#) describes the fields on the Exposure Analyzer page and the Device Details page.

On the Exposure Analyzer page, you can generate EOL reports and PBN reports for a particular device and export the reports in Excel format. An EOL report includes the following information: 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.

- 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
- Replacement numbers

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.

Service Insight uses two timers, one that runs every midnight, and another that runs every hour. The hourly timer initiates Service Insight to process pending EOL requests. This timer schedules when Service Insight requests for EOL and PBN information from JSS. When the number of managed devices is large, JSS sends EOL and PBN information 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 changes in Service Now while either one of these timers is running, Service Insight takes an hour to display the changes on the **Exposure Analyzer** page.

Figure 140: 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 40 on page 412 describes the icons on the exposure analyzer page.

Table 40: Exposure Analyzer Page Icon Descriptions



Icon	Description
	An EOL report is received for the device
	A PBN is received for the device.

Table 41 on page 412 describes the fields on the Exposure Analyzer page and the Device Details dialog box.

Table 41: Device Details from the Exposure Analyzer Page

Field	Description
Name	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

Table 41: Device Details from the Exposure Analyzer Page (continued)

Field	Description
Connection Status	<p>Connection status of the device in Junos Space.</p> <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	Parts of the device identified as EOL
Matching PBNs	Number of PBNs received for the device
Last updated	Date and time the EOL or PBN status of device was last updated

Benefits of Exposure Analyzer

Exposure Analyzer provides you the following information: You can view the number of EOL parts and PBNs

- Number of EOL parts in a device
- Number of known issues to which a device is susceptible

This information helps you take proactive measures to mitigate downtime of your network because of EOL parts or known issues.

Actions That You Can Perform From the Exposure Analyzer Task

You can perform the following actions from the **Exposure Analyzer** task:

- View devices that have an EOL part or a PBN notification associated with it
- Generate EOL reports; see [“Generating EOL Reports” on page 413](#) for details.
- Generate PBN reports; see [“Generating PBN Reports” on page 415](#) for details.
- View PBNs that are applicable to devices in your network; see [“Viewing PBNs for a Device” on page 419](#) for details.

- See Also**
- [Service Insight Targeted PBNs Overview on page 430](#)
 - [Service Insight Notifications Overview on page 435](#)

Generating EOL Reports

Junos Space Service insight displays devices that have one or more parts nearing End-of-Life (EOL) on the Exposure Analyzer page. You can generate an EOL report for such devices and export the report to 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.

Starting in Service Insight Release 16.1R1, the Generate EOL Report page provides the Organization and Device Group drop-down menus to select the organization and device group for which an EOL report is to be generated.

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

By default, Service Insight has the check box cleared and stores the EOL reports in the Service Insight database.

5. Enter a name for the EOL report.

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

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

- To generate EOL report for a particular organization or device group,
 - a. Click **All devices**.

Organization and Device groups drop down menu are displayed.

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

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

7. Enter the e-mail address of one or more users 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.

8. To schedule a time for generating the report, select the **Schedule at a later time** check box and set the date and time for the EOL report to be generated.
9. 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.
10. Click **Submit**.
The Job Information dialog box displays a job ID link for the generated report.
11. 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.
12. 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.

- See Also**
- [Service Insight EOL Reports Overview on page 420](#)
 - [Generating EOL Reports on page 413](#)
 - [Regenerating EOL Reports on page 423](#)
 - [Deleting EOL Reports on page 423](#)

Generating PBN Reports

Junos Space 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 schedule a time for generating PBN reports. Service Insight identifies devices for which PBNs received from JSS are applicable and displays those devices on the Service Insight provides the Generate PBN Reports action on the Exposure Analyzer page to generate PBN reports.

A PBN report contains the following information:

- Title of the PBN
- Duration for which the PBN report is generated
- Date and time the PBN report was created
- Date and time the PBN report was last regenerated
- User who created the PBN report
- Number of devices included in the PBN report
- Hostnames of devices included in the PBN report

- Users to whom Service Insight sends the PBN report
- Number of devices impacted by the PBN
- Status of mailing the PBN report to users

Starting in Service Insight Release 15.1R1, you can generate and regenerate PBN reports based on PBN issue date. Service Insight provides the *Start Date and time* and *End Date and time* options on the Generate PBN Reports and Regenerate PBN Reports pages to define the PBN issue date for which you want to generate a PBN report.

Starting in Service Insight Release 16.1R1, the Generate PBN Report page provide the Organization and Device Group drop-down menus to select the organization and device group for which a PBN report is to be generated.

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** list, select **Generate PBN Reports**. Alternatively, right-click and select **Generate PBN Reports**.

The **Generate PBN Report** dialog box appears as shown in [Figure 141 on page 417](#).

Figure 141: 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

☒ **PBN Issue date**

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:
 - To generate PBN report for a particular organization or device group,
 - a. Click **All devices**.
Service Insight displays the Organization and Device Group drop-down list.

- b. From the **Organization** or **Device Group** drop-down list, select the organization or device group for which you want to generate the PBN report.
- To generate PBN report for devices selected in step 2, click **Selected devices shown below**.
7. For the **Send Email To:** option, enter the e-mail address of the user to whom the PBN report must be sent.

To add and delete users who must receive the e-mail, use the **Add Email** and **Delete** buttons, respectively. By default, the **Send Email To** list contains the e-mail address of the logged-in user.
8. (Optional) Under the **PBN issue date** option, select values for **Start Date and time** and **End Date and time** to generate a report of the devices affected by PBNs issued during the selected time period.



NOTE:

- If you do not specify a Start Date and time and End Date and time, managed devices in your network affected by all the PBNs issued by Juniper Support Systems (JSS) since the inception of JSS are reported.
 - If you select only the start date and time, the devices in your network affected by all the PBNs issued from the selected Start Date and time till you generate the report are included in the report.
 - If you select only the End Date and time, the devices in your network affected by all the PBNs issued by JSS since its inception and till the selected end date and time are included in the report.
-
9. (Optional) To schedule a time for generating the report, select the **Schedule at a later time** check box and set the date and time for Service Insight to generate the PBN report.
 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** after selecting the required options.

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

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

12. 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.

- See Also**
- [Service Insight PBN Reports Overview on page 425](#)
 - [Regenerating PBN Reports on page 427](#)
 - [Exporting PBN Reports on page 426](#)
 - [Deleting PBN Reports on page 427](#)

Viewing PBNs for a Device

Junos Space Service Insight lets you can view the list of PBNs that are associated with upto 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 you want to view PBNs. 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 devices that you selected.

- See Also**
- [Exposure Analyzer Overview on page 410](#)
 - [Service Insight Targeted PBNs Overview on page 430](#)
 - [Service Insight Notifications Overview on page 435](#)

Managing EOL Reports

- [Managing EOL Reports on page 419](#)

Managing EOL Reports

- [Service Insight EOL Reports Overview on page 420](#)
- [Exporting EOL Reports on page 421](#)

- [Deleting EOL Reports on page 423](#)
- [Regenerating EOL Reports on page 423](#)

Service Insight EOL Reports Overview

The EOL Reports page (**Insight Central > EOL Reports**) displays the End of Life (EOL) reports that you generate by using the Generate EOL Report action on the Exposure Analyzer page. [Figure 142 on page 420](#) shows the EOL Reports page.

Figure 142: 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

To view an EOL report, double-click a report. The EOL Report Details page appears.

[Table 42 on page 420](#) describes the fields on the **EOL Reports** page and the **EOL Report Detail** dialog box.

Table 42: 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	Number of devices that were selected to generate the EOL report. Clicking the number takes you to the Exposure Analyzer page which displays only the devices with EOL parts.
Devices with EOL parts	Number of devices with parts for which end-of-life is announced or is in the process of being announced. The EOL date of a part specifies the date when Juniper Networks announced the end-of-life of the part.
End of Life Announce parts	Number of parts in the devices in the EOL report for which EOL dates are announced.

Table 42: EOL Reports Page and EOL Report Detail Dialog Box Fields Description (continued)

Field	Description
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 does 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>
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>

Associated Actions

You can perform the following actions related to **EOL Reports**:

- Export EOL reports; see [“Exporting EOL Reports” on page 421](#) for details.
- Regenerate EOL reports; see [“Regenerating EOL Reports” on page 423](#) for details.
- Delete EOL reports; see [“Deleting EOL Reports” on page 423](#) for details.

See Also [Generating EOL Reports on page 413](#)

Exporting EOL Reports

Junos Space Service Insight provides the Export EOL Reports option in the Actions list on the EOL Reports page to export an EOL report to an Excel file. Service Insight exports 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
- Announcement Type: Indicates if the device component is end of sale, end of life, or if the component is RoHS compliant and available restrictedly.
- End of Sale Date: 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: 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: Specifies the last day the hardware engineering in Juniper Networks will support the part
- End of Service Date: 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
- Quantity: The number of units to be replaced
- Replacement Model Description: The description of the component that can replace the outdated part in the product
- RoHS Compliance: Indicates if the part is RoHS compliant or not



NOTE: Starting Service Insight Release 17.1R1, AnnouncementType, Replacement Model Description, and RoHS Compliance columns are added to the EOL report.

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 an Excel file.

3. Select **Export EOL Reports** from either the **Actions** list or the right-click menu. The **Export EOL Report** dialog box appears.
4. Click the **Click here to download EOL reports** link and save the file to your local file system.

- See Also**
- [Service Insight EOL Reports Overview on page 420](#)
 - [Generating EOL Reports on page 413](#)
 - [Regenerating EOL Reports on page 423](#)
 - [Deleting EOL Reports on page 423](#)

Deleting EOL Reports

Junos Space Service Insight provides the Delete action in the Actions list on the EOL Reports page. 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**. Service Insight deletes the selected EOL reports from the database and removes them from the **EOL Reports** page.

- See Also**
- [Generating EOL Reports on page 413](#)
 - [Service Insight EOL Reports Overview on page 420](#)

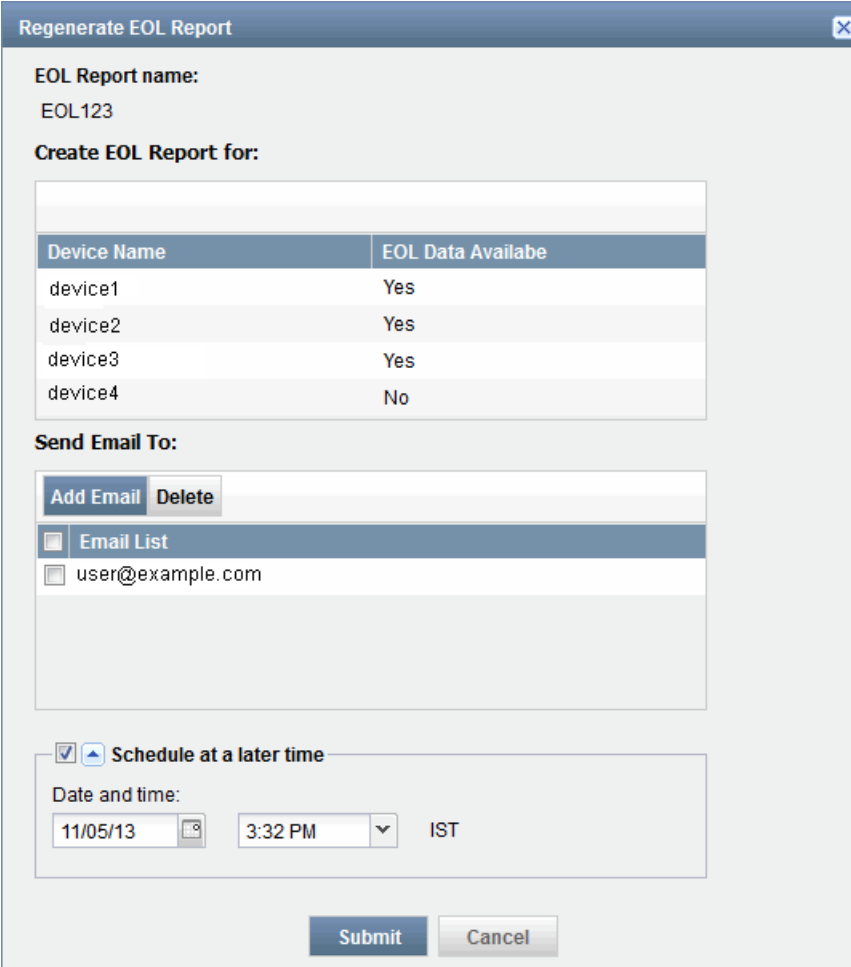
Regenerating EOL Reports

Junos Space Service Insight provides the Regenerate EOL Reports option in the Actions list on the EOL Reports page. 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 143 on page 424](#).

Figure 143: 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 two 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" section with a checkbox and the email "user@example.com", and a "Schedule at a later time" checkbox with a date/time picker set to 11/05/13 at 3:32 PM IST.
- Buttons:** "Submit" and "Cancel" at the bottom.

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.

- See Also**
- [Service Insight EOL Reports Overview on page 420](#)
 - [Generating EOL Reports on page 413](#)
 - [Exporting EOL Reports on page 421](#)

Managing PBN Reports

- [Service Insight PBN Reports Overview on page 425](#)
- [Exporting PBN Reports on page 426](#)
- [Deleting PBN Reports on page 427](#)
- [Regenerating PBN Reports on page 427](#)

Service Insight PBN Reports Overview

The **PBN Reports** page (**Insight Central > PBN Reports**) displays the PBN reports that you generate as shown in [Figure 144 on page 425](#). 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 144 on page 425](#).

Figure 144: 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 43 on page 425](#) describes the fields on the PBN Reports page and the PBN Report Detail dialog box.

Table 43: 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

Table 43: PBN Reports Page and PBN Report Detail Dialog Box Fields Description (continued)

Field	Description
PBNs Issued From	Date selected in the report from when PBNs were issued
PBNs Issued till	Date selected in the report till when PBNs were issued
Created By	Name of the user who created the PBN report
Devices Selected	Number of devices that were selected to generate the PBN report
Devices Matching PBNs	Devices for which the PBNs are applicable

Associated Actions

You can perform the following actions related to the **PBN Reports**:

- Export PBN reports; see [“Exporting PBN Reports” on page 426](#) for details.
- Regenerate PBN reports; see [“Regenerating PBN Reports” on page 427](#) for details.
- Delete PBN reports; see [“Deleting PBN Reports” on page 427](#) for details.

See Also • [Generating PBN Reports on page 415](#)

Exporting PBN Reports

Junos Space Service Insight provides the Export PBN Report option in the Actions list of the PBN Reports page to export the information in a PBN report to an Excel file.

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.

See Also • [Service Insight PBN Reports Overview on page 425](#)

- [Generating PBN Reports on page 415](#)
- [Regenerating PBN Reports on page 427](#)
- [Deleting PBN Reports on page 427](#)

Deleting PBN Reports

Junos Space Service Insight provides the delete option in the Actions list of the PBN Reports page to 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**.
Service Insight deletes selected PBN reports from the database and removes it from the the **PBN Reports** page.

- See Also**
- [Generating PBN Reports on page 415](#)
 - [Service Insight PBN Reports Overview on page 425](#)

Regenerating PBN Reports

Junos Space Service Insight provides the Regenerate PBN Reports option on the Actions list to regenerate reports on proactive bug notifications (PBNs) to get information about devices impacted by latest PBNs issued by Juniper Support Systems (JSS). Service Insight provides the Generate PBN Reports action on the Exposure Analyzer page to generate PBN reports.

Starting in Service Insight Release 15.1R1, you can generate and regenerate PBN reports based on PBN issue date. Service Insight provides the *Start Date and time* and *End Date and time* options on the Generate PBN Reports and Regenerate PBN Reports pages to define the PBN issue date for which you want to generate a PBN report.

Starting in Service Insight Release 16.1R1, the Generate PBN Reports and Generate EOL Reports page provide the Organization and Device Group drop-down list to select the organization and device group for which a PBN or EOL report is to be generated.

To regenerate PBN reports:

1. From the Service Insight navigation tree, select **Insight Central > PBN Reports**.

PBN reports are displayed.

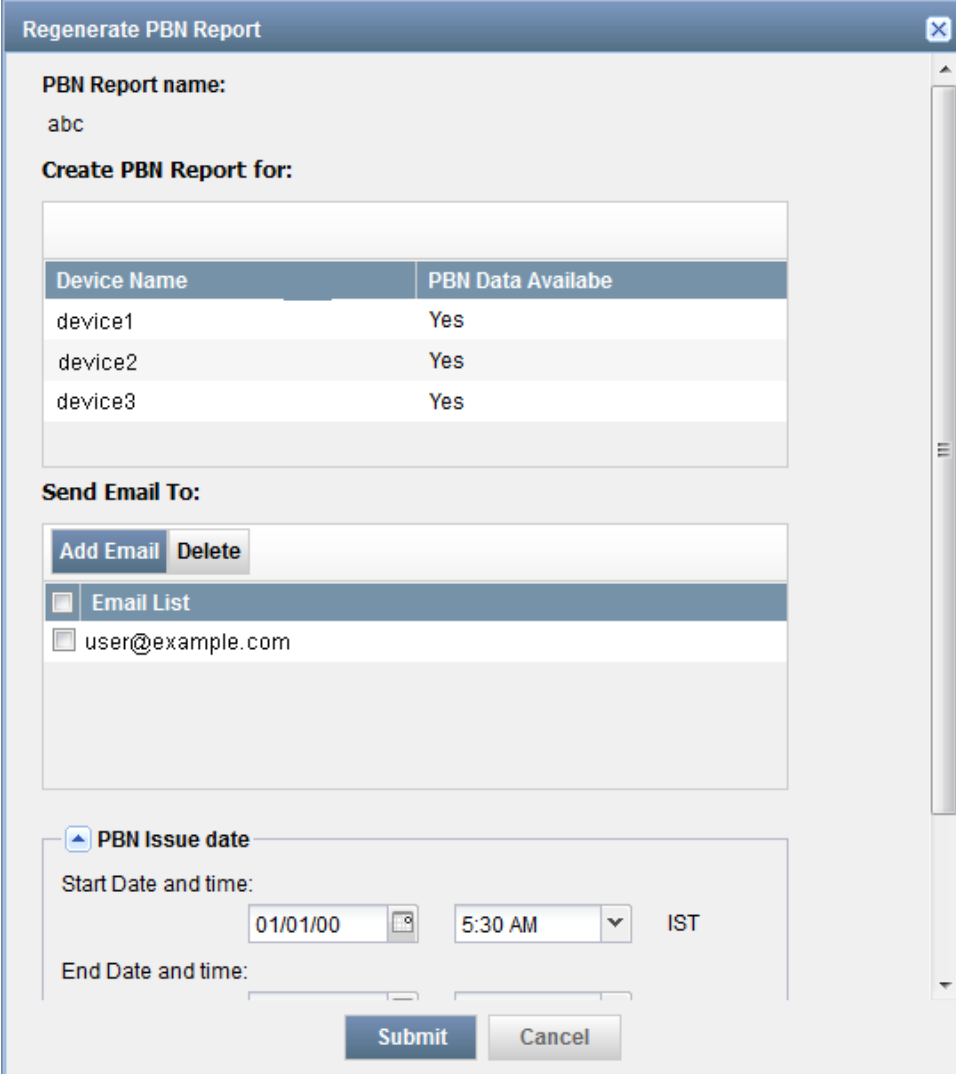
2. Select the PBN report that you want to regenerate.

3. From the **Actions** list, 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 for which the PBN report is to be regenerated, and the e-mail addresses to which notification is sent when the PBN report is generated or regenerated.

[Figure 145 on page 428](#) displays the Regenerate PBN Report dialog box..

Figure 145: Regenerate PBN Report Dialog Box



The dialog box is titled "Regenerate PBN Report" and contains the following sections:

- PBN Report name:** abc
- Create PBN Report for:** A table with two columns: "Device Name" and "PBN Data Available".

Device Name	PBN Data Available
device1	Yes
device2	Yes
device3	Yes
- Send Email To:** Includes "Add Email" and "Delete" buttons, an "Email List" section with a checkbox and the email "user@example.com", and an empty text area for additional emails.
- PBN Issue date:** Includes "Start Date and time:" with a date field (01/01/00), a time field (5:30 AM), and a time zone dropdown (IST). It also includes an "End Date and time:" section with empty fields.
- Buttons:** "Submit" and "Cancel" buttons at the bottom.

4. (Optional) To add or delete users who must receive e-mail notifications when the PBN report is regenerated, use the **Add Email** and **Delete** buttons respectively.
5. (Optional) Under the **PBN issue date** option, select values for **Start Date and time** and **End Date and time** to generate a report of the devices affected by PBNs issued during the selected time period.

**NOTE:**

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

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.

- See Also**
- [Service Insight PBN Reports Overview on page 425](#)
 - [Exporting PBN Reports on page 426](#)
 - [Generating PBN Reports on page 415](#)
 - [Deleting PBN Reports on page 427](#)

Managing PBNs

- [Managing PBNs on page 429](#)

Managing PBNs

- [Service Insight Targeted PBNs Overview on page 430](#)
- [Scanning PBNs for Impact on Devices on page 432](#)
- [Flagging PBNs to Users on page 432](#)
- [Assigning an Owner to a PBN on page 433](#)

- Deleting PBNs on page 434
- E-Mailing PBNs on page 434

Service Insight Targeted PBNs Overview

Junos Space 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 for Juniper Support Systems (JSS) to communicate information collected while helping one customer fix issues, to another customer who could face similar issues.

Using information, which was collected when issues were reported to JSS, JSS identifies devices on your network with similar conditions. When devices on your network are identified to have similar configuration as those devices on which issues were found, JSS identifies the PBNs for these devices. Service Insight picks up these PBNs once every 24 hours and displays them on the **Targeted PBNs** page (**Insight Central > Targeted PBNs**).

These PBNs keep you aware of the possible impacts the issues identified can have on your network and also the workarounds to fix the issue. The workarounds suggest temporary fixes and instructions that you can follow to protect your network.

In Service Insight, you can view targeted PBNs on the Targeted PBNs page as shown in [Figure 14-6 on page 430](#).

Figure 146: Targeted PBNs Page

SPACE

User super logged in Domain: Global Fri Jul 15 2016 08:57 AM IST

Applications Insight Central Targeted PIRNs

Service Insight Actions - Updated Time 0 Item Selected

Title	Issue Date	Updated Time	Jumper ID	Organization	Resolved In
CORE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 2, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:14 AM IST	10000002	Test_Org	14ZR1
CONE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 2, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:14 AM IST	10000002	Test_Org	14ZR1
CORE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 2, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:14 AM IST	10000002	Test_Org	14ZR1
CONE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 2, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:14 AM IST	10000002	Test_Org	14ZR1
CORE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 8, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:13 AM IST	10000007	Test_Org	14ZR1
CONE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 8, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:14 AM IST	10000007	Test_Org	14ZR1
test	Jun 20, 2016 12:30:00 PM IST	Jul 13, 2016 5:30:16 AM IST	10000060	Test_Org	13JRC-08 13JRS-03 13JR7 14 IR5 15 JR1
test	Jun 20, 2016 12:30:00 PM IST	Jul 13, 2016 5:30:16 AM IST	10000060	Test_Org	13JRC-08 13JRS-03 13JR7 14 IR5 15 JR1
MFTM might not always be able to install its own forwarding logic	Jun 22, 2016 12:30:00 PM IST	Jul 12, 2016 8:33:13 AM IST	10000229	Test_Org	12JRB 13 IRS 13JRM 13JRA 14 IR2 14ZR1
test	Jun 22, 2016 12:30:00 PM IST	Jul 13, 2016 5:30:16 AM IST	10000060	Test_Org	13JRC-08 13JRS-03 13JR7 14 IR5 15 JR1
Clients lose connectivity because probe ARP packets are dropped by Dynamic ARP Inspection (DAI) check.	Jun 23, 2016 12:30:00 PM IST	Jul 14, 2016 9:33:32 AM IST	874106	new_testing_org	
CORE-POT Estart OTN OTN payload PRBS support for Estart test	Jun 23, 2016 12:30:00 PM IST	Jul 14, 2016 9:33:32 AM IST	10000007	new_testing_org	14ZR1
On OfflineOnline code of a 40GE QSFP use (PCHMAC), a 40G interface ports Physical Link might remain down	Jun 23, 2016 12:30:00 PM IST	Jul 14, 2016 9:33:33 AM IST	10026888	new_testing_org	14R3-G1 14 R4
[SRST] After exhaustion due to multiple port sessions stuck in LACP_Ack state	Jun 23, 2016 12:30:00 PM IST	Jul 14, 2016 9:33:33 AM IST	10298756	new_testing_org	12 I14A-O5 12 I14AF-O35 12 I14AT-O5 12 JRC-04 12 JRC9 12 J2AB-O15 13JRT 13J2T-O25

Page 1 of 2

A targeted PBN contains the fields listed in [Table 44 on page 430](#). On the targeted PBNs page, you can filter and view PBNs based on organization. Using a targeted PBN, you can scan for devices impacted by the vulnerabilities described in the targeted PBN in an organization and list the devices; for more information, see “[Scanning PBNs for Impact on Devices](#)” on page 432.,

Table 44: Targeted PBNs Field Descriptions

Field	Description
Title	Title of the PBN, which is a short description of the issue found

Table 44: Targeted PBNs Field Descriptions (continued)

Field	Description
Issue Date	Date and time when the issue was recorded
Updated Time	Date and time the PBN was last updated
Juniper ID	Unique ID specified by Juniper Networks that is used to identify the PBN
Organization	Organization to which the PBN is applicable
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
Work Around	Temporary fix for the problem
Instructions	Additional information that you can follow
Relevances	Devices that could be impacted by the problem described by the PBN
Customer Impact	Impact of the bug on the customer network
Impact Probability	Probability that the bug would impact the network
Owner	User who has been assigned ownership of the PBN using Service Insight
Flagged to Users	Users who were notified about the PBN using Service Insight

Associated Actions

You can perform the following actions related to targeted PBNs:

- View targeted PBNs received from JSS
- Scan for devices that are impacted by PBNs; see [“Scanning PBNs for Impact on Devices” on page 432](#) for details.
- Flag PBNs to users; see [“Flagging PBNs to Users” on page 432](#) for details.
- E-mail PBNs to users; see [“E-Mailing PBNs” on page 434](#) for details.
- Assign an owner to a PBN; see [“Assigning an Owner to a PBN” on page 433](#) for details.
- Delete one or more PBNs; see [“Deleting PBNs” on page 434](#) for details.

See Also • [Exposure Analyzer Overview on page 410](#)

Scanning PBNs for Impact on Devices

Junos Space Service Insight provides the Scan for Impact option in the Actions list to identify the devices within an organization that could be impacted by the vulnerabilities described in a targeted PBN.

To scan PBNs and view the impacted devices:

1. From the **Service Insight** taskbar, select **Insight Central > Targeted PBNs**.

The Targeted 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 click **Scan for Impact**.

The **Scan for Impact** dialog box appears requesting confirmation for scanning devices that would be impacted by the selected PBN.

4. Click **Confirm**

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.

- See Also**
- [Exposure Analyzer Overview on page 410](#)
 - [Assigning an Owner to a PBN on page 433](#)

Flagging PBNs to Users

Junos Space Service Insight provides the Flag to Users option in the Actions list of the Targeted PBNs page to flag PBNs to Junos Space users who you think need to keep track of the PBNs or who need to receive them.

To flag PBNs to a user:

1. From the **Service Insight** navigation tree, select **Insight Central > Targeted PBNs**.

The **Targeted PBNs** page displays the list of targeted PBNs.

2. Select one or more PBNs 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. (Optional) 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. The PBN Details page appears. The PBN is flagged to users listed on the page,

- See Also**
- [Assigning an Owner to a PBN on page 433](#)
 - [E-Mailing PBNs on page 434](#)
 - [Deleting PBNs on page 434](#)

Assigning an Owner to a PBN

You can assign a PBN to a Junos Space user for looking into the issues and assessing the impact on devices.

To assign ownership of a PBN:

1. From the Service Insight navigation tree, select **Insight Central > Targeted PBNs**. The **Targeted 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 whom you want to 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. The PBN Details page appears. The Owner field displays the user responsible for the PBN.

- See Also**
- [Exposure Analyzer Overview on page 410](#)
 - [Scanning PBNs for Impact on Devices on page 432](#)
 - [E-Mailing PBNs on page 434](#)
 - [Flagging PBNs to Users on page 432](#)

Deleting PBNs

Junos Space Service Insight provides the Delete PBNs option to delete PBNs that are displayed on the Targeted PBNs page.

To delete PBNs:

1. From the Service Insight navigation tree, select **Insight Central > Targeted PBNs**.
The Targeted PBNs page displays the list of PBNs received.
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.

- See Also**
- [Exposure Analyzer Overview on page 410](#)
 - [Scanning PBNs for Impact on Devices on page 432](#)
 - [Assigning an Owner to a PBN on page 433](#)
 - [Generating PBN Reports on page 415](#)

E-Mailing PBNs

Junos Space Service Insight provides the Email PBNs to Users option to 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 **Targeted PBNs** page displays the list of PBNs received.
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.

- See Also**
- [Assigning an Owner to a PBN on page 433](#)
 - [Flagging PBNs to Users on page 432](#)
 - [Scanning PBNs for Impact on Devices on page 432](#)

Managing Notifications

- [Managing Notifications on page 435](#)

Managing Notifications

- [Service Insight Notifications Overview on page 435](#)
- [Creating and Copying a Notification on page 436](#)
- [Editing the Filters and Actions of a Notification on page 439](#)
- [Enabling and Disabling Notifications on page 439](#)
- [Deleting Notifications on page 440](#)

Service Insight Notifications Overview

In Junos Space 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 from JSS.
 - **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**—List of user e-mail IDs and SNMP trap destinations to which the notifications must be sent when the event occurs.

The Notifications page (**Insight Central > Notifications**) enables you to manage these notifications. This page displays the notifications chronologically by name, owner, status, and trigger. [Table 45 on page 436](#) provides more information about the fields on the **Notifications** page.

Table 45: Description of Fields on Notifications Page

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

On the Service Insight Notifications page, you can perform the following tasks:

Associated Actions

You can perform the following actions related to notifications:

- Create and copy notifications; see [“Creating and Copying a Notification” on page 436](#) for details.
- Edit filters and actions of a notification; see [“Editing the Filters and Actions of a Notification” on page 439](#) for details.
- Enable or disable notifications; see [“Enabling and Disabling Notifications” on page 439](#) for details.
- Delete notifications; see [“Deleting Notifications” on page 440](#) for details.

See Also • [Service Insight Targeted PBNs Overview on page 430](#)

Creating and Copying a Notification

Junos Space Service Insight provides the Create Notifications option in the Notifications task to create notifications by specifying when you want Service Insight to send notifications and the recipients of the notification. While creating the notification, you can define filters that specify the trigger events, and the recipients and the destinations for SNMP traps to which Service Insight should send the notifications.

This topic provides procedures for creating and copying notifications.

- [Creating a Notification on page 437](#)
- [Copying a Notification on page 437](#)

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 46 on page 438](#).

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 can 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

You can copy a notification policy to create a similar notification policy with few differences.

To copy a notification policy:

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

The **Notifications** page displays the notifications. For descriptions about the fields on this page see [Table 46 on page 438](#).

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 on the Notifications page.

Table 46: 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 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.

See Also

- [Service Insight Targeted PBNs Overview on page 430](#)
- [Enabling and Disabling Notifications on page 439](#)

Editing the Filters and Actions of a Notification

You can edit notification parameters, such as the applied filters, and the actions to be taken by using the Edit Filters and Actions option in the Actions list on the Notifications page.

To edit a notification:

1. From the Service Insight navigation tree, select **Insight Central > Notifications**.
The **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.

- See Also**
- [Service Insight Targeted PBNs Overview on page 430](#)
 - [Creating and Copying a Notification on page 436](#)
 - [Enabling and Disabling Notifications on page 439](#)

Enabling and Disabling Notifications

Junos Space Service Insight provides the Enable/Disable Notifications option on the Actions list of the Notifications page to 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 Notifications page and can be enabled whenever required.

A notification is sent for an event only when the notification is enabled.

When a public tag that is set as a filter level for a notification is deleted, the notification continues to be displayed on the 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 **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.

- See Also**
- [Service Insight Targeted PBNs Overview on page 430](#)
 - [Creating and Copying a Notification on page 436](#)

Deleting Notifications

Junos Space Service Insight provides the Delete option on the Notifications page to delete notifications.

To delete notifications:

1. From the Service Insight navigation tree, select **Insight Central > Notifications**.
The **Notifications** page displays the notifications.
2. Select one or more 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.
Service Insight deletes the notifications and removes them from the Notifications page.

- See Also**
- [Service Insight Targeted PBNs Overview on page 430](#)
 - [Creating and Copying a Notification on page 436](#)
 - [Enabling and Disabling Notifications on page 439](#)

CHAPTER 11

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 Associated 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.

Appendix

- [Sample Perl Script for Incident and Auto Submit Filters on page 457](#)

Sample Perl Script for Incident and Auto Submit Filters

The following is a sample Perl script for incident and auto submit filters implemented by using Perl module:

```
#!/usr/bin/perl
use lib qw(/var/cache/jboss/SN/AdvancedFilters /usr/nma/lib
/usr/lib/perl5/vendor_perl/5.8.8);
use MyModule; #Custom_User_Module
use NmaUtil;
use filterUtilV1;

#Input arguments passed from Service Now
$eventType = $ARGV[0];
$deviceHostName = $ARGV[1];
$problemSynopsis = $ARGV[2];
$problemDescription = $ARGV[3];
$osPlatform = $ARGV[4]; # Argument not present in Incident Entity table;
present only as part of JMB
$entity = $ARGV[5];
$junosVersion = $ARGV[6];
$eventTime = $ARGV[7];
$deviceId = $ARGV[8];

#Supported values
[devicePlatform,device_node,customerTrackingNumber,hostName,problemDesc,
problemSynopsis,defectDesc,defectType,prbIdentifier,junosVersion,
occurredTimeStartRange,occurredTimeEndRange]
my %incident_hash = ('hostName'=>'RouterName',
                    'occurredTimeStartRange'=> '2018-01-23 10:47:47'
                    );

print "MyModule = $MyVariable"; #Using user variables inside MyModule
print "CheckStatus = ". Verify_CheckStatus(); #Calling user Functions inside
MyModule

#getExistingIncidents() will return
[PRbTime,Priority,Severity,defectDesc,defectType,device_node,hostName,prbIdentifier,problemDesc,problemSynopsis,junosVersion]
my $incidents = filterUtilV1::getExistingIncidents(%incident_hash);

print "\n$incidents\n";
```

```
if ( $deviceHostName eq 'RouterName' ){  
    print "\ntrue";  
}  
else{  
    print "\nfalse";  
}
```



NOTE: Do not change the ARG value assigned to a JMB attribute.
