



Junos[®] Space

Network Management Platform User Guide

Release

13.1



Modified: 2016-06-23

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

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

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

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

Junos® Space Network Management Platform User Guide

13.1

Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xxxi
	Documentation and Release Notes	xxxi
	Documentation Conventions	xxxi
	Documentation Feedback	xxxiii
	Requesting Technical Support	xxxiv
	Self-Help Online Tools and Resources	xxxiv
	Opening a Case with JTAC	xxxiv
Part 1	Junos Space User Interface	
Chapter 1	Getting Started	3
	Logging In to Junos Space	3
	Changing User Passwords	4
	Using the Getting Started Assistants	5
	Accessing Help	6
	Logging Out	6
Chapter 2	Understanding the Junos Space User Interface	9
	Junos Space User Interface Overview	9
	The Main Display	9
	Banner	10
	Task Tree	11
	Main Window	12
	Application Dashboard	13
	Dashboard Gadgets	13
	Task Group (Workspace) Statistics	14
	Inventory Page	15
	Banner Icon Buttons	16
	Sorted-by Indicator	16
	Show or Hide Columns	17
	Filter Submenus	17
	Search Field	18
	Actions Menu	19
	Paging Controls	19
	Global Search	20
	Navigating the Junos Space User Interface	26
	Navigating the Task Tree: The Devices Workspace	26
	Filtering Inventory Pages	27

Part 2	Devices	
Chapter 3	Device Management Overview	35
	Device Management Overview	35
	Viewing Device Statistics	36
	Viewing the Number of Devices by Platform	37
	Viewing Connection Status for Devices	37
	Viewing Devices by Junos OS Release	38
	Device Inventory Management Overview	40
	Viewing Managed Devices	41
	Viewing Devices	42
	Viewing Devices and Logical Systems with QuickView	46
	Understanding How Junos Space Automatically Resynchronizes Managed	
	Devices	47
	Network as System of Record	47
	Junos Space as System of Record	49
	Troubleshooting Devices	49
Chapter 4	Device Configuration	51
	Viewing Active Configuration	52
	Adding Configuration Filters	53
	Modifying Device Configuration Overview	53
	Selecting the Device and the Configuration Perspective	54
	Modifying the Configuration on the Device	55
	Modifying Unmanaged Device Configuration	57
	Reviewing and Deploying the Device Configuration	57
	Viewing the Device Configuration Changes	58
	Validating the Configuration on the Device	59
	View the Device-Configuration Validation Report	59
	Excluding or Including a Group of Configuration Changes	60
	Deleting a Group of Configuration Changes	60
	Approving the Configuration Changes	61
	Rejecting the Configuration Changes	61
	Deploying the Configuration Changes	62
	Configuration Guides Overview	63
	Saving the Configuration Created using the Configuration Guides	63
	Deploying the Configuration Created using the Configuration Guides	64
	Previewing the Configuration Created using the Configuration Guides	64
	Resolving Out-of-Band Configuration Changes	65
	Viewing the Configuration Change Log	65
	Managing Configuration Changes	66
	Viewing Configuration Change Log	66
	Viewing Assigned Shared Objects	68
	Viewing Template Deployment (Devices)	70
Chapter 5	Device Inventory	73
	Viewing Physical Inventory	73
	Displaying Service Contract and EOL Data in the Physical Inventory Table	75
	Viewing Physical Interfaces	76
	Viewing Logical Interfaces	77

	Viewing and Exporting License Inventory	80
	Viewing and Exporting Software Inventory	84
	Exporting Physical Inventory Information	86
	Viewing Associated Scripts	87
	Executing Scripts on a Physical Inventory Component	87
	Executing Scripts on a Physical Interface	88
	Executing Scripts on a Logical Interface	89
	Applying CLI Configlets to a Physical Inventory Element	90
	Applying CLI Configlets to a Physical Interface	90
	Applying CLI Configlets to a Logical Interface	91
Chapter 6	Device Operations	93
	Deleting Devices	93
	Resynchronizing Managed Devices With the Network	94
	Using Looking Glass	96
	Understanding Logical Systems for SRX Series Services Gateways	97
	Creating a Logical System (LSYS)	98
	Deleting Logical Systems	99
	Viewing the Physical Device for a Logical System	99
	Viewing Logical Systems for a Physical Device	100
	Putting a Device in RMA State and Reactivating Its Replacement	101
	Putting a Device in RMA State	101
	Reactivating a Replacement Device	102
	Applying CLI Configlets to a Device	103
	Executing Scripts on Devices	103
	Executing Scripts on Devices Remotely with JUICE	104
Chapter 7	Device Access	105
	Secure Console Overview	105
	Connecting to a Device From Secure Console	106
	Connecting to a Managed Device from the Device Management Page	106
	Connecting to an Unmanaged Device from the Device Management Page	107
	Connecting to a Managed or Unmanaged Device from the Secure Console Page	108
	Launching a Device's Web UI	109
	Changing Device Credentials	110
	Key-based Authentication Overview	111
	Generating and Uploading Authentication Keys to Devices	112
	Generating Keys	112
	Uploading Keys to Devices for the First Time	113
	Upload Keys on Managed Devices that have Conflicting keys with Junos Space	114
	Verifying Device Key Status	115
	Resolving Key Conflicts	116
	Changing Device Authentication from Password-based to Key-based Authentication	116

Chapter 8	Device Monitoring	119
	Viewing and Managing Alarms	119
	Viewing Alarms	120
	Acknowledging Alarms	122
	Clearing Alarms	122
	Escalating Alarms	122
	Unacknowledging Alarms	122
	Viewing Acknowledged Alarms	123
Chapter 9	Custom Attributes	125
	Adding Custom Labels	125
	Adding Custom Labels for a Device	125
	Adding Custom Labels for Physical Inventory	126
	Adding Custom Labels for a Physical Interface	127
	Adding Custom Labels for a Logical Interface	127
	Managing Custom Labels	128
	Modifying Custom Labels	128
	Deleting Custom Labels	128
Chapter 10	Discover Devices	131
	Device Discovery Overview	131
	Discovering Devices	132
	Specifying Device Targets	133
	Specifying Probes	135
	Specifying Credentials	136
Chapter 11	Deployed Devices	139
	Adding Deployed Devices	139
	Add Deployed Devices Wizard Overview	141
	Managing Deployed Devices	142
	Viewing the Details of a Task Instance	142
	Viewing the Device Status	142
	Deleting a Task Instance	143
	Downloading Management CLI Commands	143
	Adding SRX Series Devices Overview	143
	Adding Devices	145
	Creating a Deployment Instance	145
	Adding a Deployment Instance by Importing a CSV File	146
	Adding a Deployment Instance Manually	147
	Working with Rows and Columns	147
	Working with Configlets	149
	Deploying Device Instances	149
	Viewing the Details of a Deployment Instance	150
	Viewing the Device Status	150
	Deleting a Deployment Instance	150
	Downloading Configlets	150
	Searching for a Deployment Instance	151
Chapter 12	Unmanaged Devices	153
	Adding Unmanaged Devices	153

Chapter 13	Secure Console	157
	Configuring SRX Device Clusters in Junos Space	157
	Configuring a Standalone Device from a Single-node Cluster	157
	Configuring a Standalone Device from a Two-Node Cluster	159
	Configuring a Primary Peer in a Cluster from a Standalone Device	160
	Configuring a Secondary Peer in a Cluster from a Standalone Device	161
Chapter 14	Manage Device Adapter	165
	Worldwide Junos OS Adapter Overview	165
	Installing the Worldwide Junos OS Adapter	166
	Installing the wwadapter Image	166
	Connecting to ww Junos OS Devices	167
Chapter 15	Upload Keys to Devices	169
	Key-based Authentication Overview	169
	Generating and Uploading Authentication Keys to Devices	170
	Generating Keys	170
	Uploading Keys to Devices for the First Time	170
	Upload Keys on Managed Devices that have Conflicting keys with Junos Space	172
	Verifying Device Key Status	173
Part 3	Device Templates	
Chapter 16	Overview	177
	Device Templates Overview	177
	Device Templates Overview	178
	Device Templates Workflow	181
	Viewing Statistics for Templates and Definitions	181
	User Privileges in Device Templates	182
	Changing Template Definition States	182
Chapter 17	Template Definitions	183
	Manage Definitions	183
	Managing Template Definitions	183
	Publishing and Unpublishing a Template Definition	184
	Modifying a Template Definition	185
	Viewing Template Definition Inventory	185
	Cloning a Template Definition	186
	Deleting a Template Definition	187
	Exporting a Template Definition	187
	Create Definition	188
	Creating a Template Definition Overview	188
	Creating a Template Definition	189
	Selecting the Device Family and Naming the Definition	189
	Creating Configuration Pages	190
	Determining Editable Parameters	192
	Filling in the General Tab	193
	Filling in the Description Tab	195
	Filling in the Validation Tab	196

	Filling in the Advanced Tab	197
	Specifying Default Values for Configuration Options	198
	Finding Configuration Options	199
	Specifying Device-Specific Values in Definitions	200
	Working with Rules	203
	Manage CSV Files	204
	Managing CSV Files	204
	Import Definitions	205
	Importing Template Definitions Overview	205
	Importing a Template Definition	206
Chapter 18	Templates	209
	Manage Templates	209
	Managing Templates Overview	209
	Template States	210
	Filtering and Searching Templates	210
	Device Template Detailed Information	210
	Template Actions	211
	Deleting a Template	212
	Deploying a Template	213
	Modifying a Template	214
	Undeploying a Template	215
	Viewing Template Deployment (Device Templates)	217
	Auditing Template Configuration	219
	Assigning a Template to a Device	220
	Unassigning a Template From a Device	221
	Creating a Template Overview	222
	Creating a Template	223
	Selecting a Template Definition	223
	Naming and Describing a Template	223
	Entering Data and Finishing the Template	224
	Deploying the Template	225
	Viewing Template Inventory	225
	Viewing Template Statistics	226
	Create Template	226
	Creating a Template Overview	227
	Creating a Template	227
	Selecting a Template Definition	227
	Naming and Describing a Template	228
	Entering Data and Finishing the Template	229
	Deploying the Template	230
Part 4	CLI Configlets	
Chapter 19	CLI Configlets Overview	233
	CLI Configlets Overview	233
	CLI Configlets Overview	233
	Configlet Variables	234
	Velocity Templates	234
	CLI Configlets Workflow	235

	Configlets User Roles	237
	Configlet Context	238
	Context of an Element	239
	Context filtering	240
	Nesting Parameters	242
Chapter 20	Managing CLI Configlets	243
	Manage CLI Configlets	243
	Managing CLI Configlets	243
	Creating CLI Configlets	244
	Viewing CLI Configlets	245
	Editing CLI Configlets	245
	Cloning CLI Configlets	245
	Deleting CLI Configlets	246
	Applying CLI Configlets	246
	Viewing CLI Configlet Statistics	247
	Viewing the Number of Configlets by Device Family	247
	Viewing the Number of Configlets by Category	248
	CLI Configlet Examples	248
	CLI Configlet Examples	248
	Example 1 - Setting the description of a physical interface	248
	Example 2 - Setting the vlan of a logical interface, where the vlan id is chosen from a predefined set of values	249
	Example 3 - Setting a description on all the interfaces of a device	250
	Example 4 - Need to set a configuration in all the PICs belonging to a device and certain configuration only on the first PIC of FPC 0	251
	Example 5 - Halting the description of a physical interface	253
Chapter 21	Configuration Views Overview	255
	Configuration View Overview	255
	Configuration View Variables	256
	Configuration View Workflow	256
	Configuration Views User Roles	257
	XML Extensions	258
Chapter 22	Managing Configuration Views	261
	Manage Configuration Views	261
	Create Configuration View	262
	View Configuration View	262
	Edit Configuration View	263
	Delete Configuration View	263
	Viewing Configuration Views Statistics	263
Chapter 23	XPath and Regex	265
	XPATH and Regex	265
	Creating Xpath and Regex	265
	Managing Xpath and Regex	266
	Modifying the Xpath and Regex	266
	Deleting the Xpath and Regex	266

Part 5	Images and Scripts	
Chapter 24	Overview	269
	Device Images and Scripts Overview	269
	User Roles	270
Chapter 25	Device Images	273
	Device Images Overview	273
Chapter 26	Scripts	275
	Scripts Overview	275
Chapter 27	Operations	279
	Operations Overview	279
Chapter 28	Script Bundles	281
	Script Bundles Overview	281
Chapter 29	Configuration: Device Images	283
	Uploading Device Images to Junos Space	283
	Staging Device Images	284
	Verifying the Checksum	286
	Deploying Device Images	286
	Viewing Device Image Deployment Results	293
	Deleting Device Images	293
	Modifying Device Image Details	294
	Viewing and Deleting MD5 Validation Results	295
	Viewing the MD5 Validation Results	295
	Deleting the MD5 Validation Results	296
Chapter 30	Configuration: Scripts	297
	Modifying a Script	297
	Modifying Script Types	298
	Comparing Script Versions	299
	Deleting Scripts	299
	Staging Scripts on Devices	300
	Viewing Associated Devices	301
	Verifying the Checksum of Scripts on Devices	302
	Enabling Scripts on Devices	304
	Disabling Scripts on Devices	306
	Removing Scripts from Devices	307
	Executing Scripts on Devices	309
	Viewing Execution Results	311
	Importing Scripts	313
Chapter 31	Configuration: Operations	315
	Creating an Operation	315
	Modifying an Operation	317
	Running an Operation	318
	Copying an Operation	319
	Deleting an Operation	320
	Exporting an Operation in TAR Format	320

	Importing an Operation	322
Chapter 32	Configuration: Script Bundles	325
	Creating a Script Bundle	325
	Modifying a Script Bundle	326
	Deleting Script Bundles	327
	Staging Script Bundles on Devices	328
	Executing Script Bundles on Devices	329
	Enabling Scripts in Script Bundles on Devices	330
	Disabling Scripts in Script Bundles on Devices	332
Chapter 33	Administration: Scripts	335
	Viewing Script Details	335
	Viewing Verification Results	336
	Exporting Scripts in Tar Format	337
Chapter 34	Administration: Operations	339
	Viewing Operations Results	339
Chapter 35	Administration: Script Bundles	341
	Viewing Device Association of the Scripts in Script Bundles	341
Chapter 36	Annotations and Examples	343
	Scripts Annotations	343
	Scripts Examples	344
Part 6	Reports and Report Definitions	
Chapter 37	Report Definitions	349
	Reports Overview	350
	Creating Report Definitions	355
	Managing Report Definitions	356
	Modify Report Definitions	356
	Cloning Report Definitions	357
	Deleting Report Definitions	357
	Viewing Report Definitions	357
Chapter 38	Reports	359
	Generating Reports	359
	Viewing Generated Reports	360
	Deleting Generated Reports	360
Part 7	Network Monitoring	
Chapter 39	Network Monitoring Overview	365
	Network Monitoring Workspace Overview	365
	Network Monitoring Reports Overview	368
	Resource Graphs	368
	Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports	368
	Database Reports	368
	Statistics Reports	368

Chapter 40	Monitoring Devices and Assets	371
	Viewing the Node List	371
	Resyncing Nodes	372
	Turning SNMP Data Collection Off and On	372
	Searching in the Network Monitoring Workspace	374
	Viewing the Dashboard	375
	Tracking and Searching for Assets	377
	Working with Topology	378
	Viewing the Nodes Without Links	379
	Viewing Alarms and Node Details for Selected Nodes	379
	Viewing Nodes with Active Alarms	380
	Managing Alarms Associated with Nodes	380
	Filtering Nodes	381
	Viewing the Topology Map with Different Layouts	381
	Viewing the Details of a Node	381
	Pinging a Node	382
	Viewing the Alarms Associated with the Node	382
	Viewing the Events Associated with the Node	383
	Viewing the Resource Graphs Associated with the Node	383
	Grouping Nodes	383
	Adding Nodes to a Group	384
	Removing a Node from a Group	384
	Viewing the Network Services Across Nodes	385
	Viewing the Details of the Network Service Across Nodes	385
Chapter 41	Working With Events, Alarms, and Notifications	387
	Viewing and Tracking Outages	387
	Viewing and Managing Events	388
	Events Landing Page	388
	Advanced Event Search	388
	Viewing the Events List	389
	Viewing Event Details	390
	Viewing and Managing Alarms	391
	Viewing Alarms	392
	Acknowledging Alarms	393
	Clearing Alarms	394
	Escalating Alarms	394
	Unacknowledging Alarms	394
	Viewing Acknowledged Alarms	394
	Viewing, Configuring, and Searching for Notifications	395
	Notification Escalation	395

Chapter 42	Working With Reports and Charts	397
	Creating Reports	397
	Creating Key SNMP Customized Performance Reports, Node Reports, Domain Reports	397
	Creating a New KSC Report from an Existing Report	398
	Viewing Reports	398
	Viewing Resource Graphs	399
	Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, Domain Reports	399
	Viewing Database Reports	400
	Sending Database Reports	400
	Viewing Pre-run Database Reports	401
	Viewing Statistics Reports	401
	Generating a Statistics Report for Export	402
	Deleting Reports	403
	Deleting Key SNMP Customized Reports	403
	Deleting Pre-run Database Reports	403
	Viewing Charts	403
Chapter 43	Managing Network Monitoring System	405
	Admin: Configuring Network Monitoring	405
	Modifying Users	405
	Network Monitoring System: System Information	406
	Notification Status	407
Chapter 44	Managing Network Monitoring Operations	409
	Configuring SNMP Community Names by IP	409
	Configuring SNMP Data Collection per Interface	410
	Managing and Unmanaging Interfaces and Services	411
	Managing Thresholds	411
	Creating Thresholds	411
	Modifying Thresholds	414
	Deleting Thresholds	415
	Selecting and Sending an Event to the Network Management System	415
	Configuring Notifications	416
	Configuring Event Notifications	416
	Configure Destination Paths	418
	Configure Path Outages	419
	Configuring Scheduled Outages	419
	Compiling SNMP MIBs	420
	Uploading MIBs	420
	Compiling MIBs	421
	Viewing MIBs	421
	Deleting MIBs	421
	Clearing MIB Console Logs	422
	Generating Event Configuration	422
	Generating a Data Collection Configuration	423

	Managing Events Configuration Files	425
	Adding New Events Configuration Files	425
	Deleting Events Configuration Files	426
	Modifying Events Configuration Files	426
	Managing SNMP Collections	427
	Add a New SNMP Collection	427
	Modify an SNMP Collection	428
	Managing Data Collection Groups	428
	Adding New Data Collection Files	428
	Deleting Data Collection Files	429
	Modifying Data Collection Files	429
Chapter 45	Managing Devices	433
	Managing Surveillance Categories	433
	Modifying Surveillance Categories	433
	Deleting Surveillance Categories	433
	Adding Surveillance Categories	433
Chapter 46	Configuring Alarm Notifications	435
	Alarm Notification Configuration Overview	435
	Basic Filtering	435
	Guidelines for Configuring Alarm Notifications	436
	Advanced Filtering	436
	Configuring Alarm Notification	438
	Configuring a Basic Filter for Alarm Notification	438
	Activating Alarm Notification Configuration Files for Basic Filtering	439
	Reloading a Filter Configuration to Apply Filter Configuration Changes	440
Part 8	Configuration Files	
Chapter 47	Manage Configuration Files	443
	Managing Configuration Files Overview	444
	User Privileges in Configuration File Management	445
	Viewing Configuration File Statistics and Inventory	446
	Deleting Configuration Files	446
	Restoring Configuration Files	447
	Comparing Configuration Files	448
	Editing Configuration Files	450
	Exporting Configuration Files	452
Chapter 48	Backup Config Files	453
	Backing Up Configuration Files	454
Part 9	Jobs	
Chapter 49	Overview	461
	Jobs Overview	461

Chapter 50	Manage Jobs	465
	Viewing Your Jobs	465
	Viewing Scheduled Jobs	466
	The View	466
	Viewing Job Types	466
	Viewing Job Status Indicators	466
	Viewing Job Details, Status, and Results	467
	Performing Manage Jobs Commands	468
	Viewing Statistics for Scheduled Jobs	469
	Viewing the Types of Jobs That Are Run	469
	Viewing the State of Jobs That Have Run	469
	Viewing Average Execution Times for Jobs	470
	Canceling a Job	470
	Viewing Job Recurrence	471
	Retrying a Job on Failed Devices	472
Chapter 51	Archive Jobs	473
	Archiving and Purging Jobs	473
	Archiving Jobs to a Local Server and Purging the Database	473
	Archiving Jobs to a Remote Server and Purging the Database	474
Part 10	Users	
Chapter 52	Manage Roles	479
	Role-Based Access Control Overview	479
	Authentication	479
	RBAC Enforcement	479
	Enforcement by Workspace	480
	RBAC Enforcement Not Supported for Getting Started Page	480
	Understanding How to Configure Users to Manage Objects in Junos Space	480
	Predefined Roles Overview	481
	Managing Roles Overview	502
	Managing Roles	503
Chapter 53	Manage User-Defined Roles	505
	Creating a User-Defined Role	505
	Modifying User-Defined Roles	506
	Deleting User-Defined Roles	507
Chapter 54	Manage Users	509
	Creating User Accounts	509
	Creating a New User Account	510
	Limiting User Sessions	513
	Disabling and Enabling Users	515
	Viewing Users	516
	Sorting Columns	517
	Displaying or Hiding Columns	517
	Filtering on Columns	518
	Viewing User Details	518

	Performing Manage User Commands	519
	Modifying a User	520
	Deleting Users	522
	Changing User Passwords	522
	Clearing User Local Passwords	523
	Viewing User Statistics	524
	Viewing the Number of Users Assigned by Role	524
Chapter 55	Manage Remote Profiles	525
	Creating a Remote Profile	525
Chapter 56	User Sessions	527
	Terminating User Sessions	527
Part 11	Audit Logs	
Chapter 57	View	531
	Junos Space Audit Logs Overview	531
	Viewing Audit Logs	532
	Viewing Audit Log Statistics	534
	Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel	536
Chapter 58	Archive / Purge	539
	Archiving and Purging Audit Logs	539
	Archiving Audit Logs To a Local Server and Purging the Database	539
	Archiving Audit Logs To a Remote Server and Purging the Database	540
Chapter 59	Export	543
	Exporting Audit Logs	543
Part 12	Administration	
Chapter 60	Overview	547
	Junos Space Administrators Overview	547
	Maintenance Mode Overview	548
	Maintenance Mode Access and System Locking	549
	Maintenance Mode User Administration	549
Chapter 61	Fabric	551
	Fabric Management	551
	Fabric Management Overview	551
	Single Node Functionality	552
	Multinode Functionality	553
	Node Function Availability	555
	Adding a Node to an Existing Fabric	556
	Viewing Nodes in the Fabric	557
	Changing Views	558
	Viewing Fabric Node Details	558

Performing Fabric Node Actions	560
Configuring Node Network Settings	561
Network Settings Configuration Guidelines	562
Changing the VIP Interface in the Same Subnet	562
Changing the Node Management IP in the Same Subnet	562
Changing the Default Gateway	562
Changing the Management IP to a Different Network	563
Adding the Device Management IP Address	563
Changing the Device Management IP Address in the Same Subnet	564
Changing the Device Management IP Address to a Different Network	564
Deleting a Device Management IP Address	564
Changing the VIP Interface to a Different Network	565
Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet	565
Changing the VIP interface of a Multi-Node Fabric to a Different Network	565
Shutting Down or Rebooting a Node From Junos Space	566
Deleting a Node	567
Understanding Overall System Condition and Fabric Load	568
System Condition	568
Fabric Load	570
Monitoring Nodes in the Fabric	570
Viewing and Modifying the SNMP Configuration for a Fabric Node	572
Starting SNMP Monitoring on Fabric Nodes	594
Stopping SNMP Monitoring on Fabric Nodes	595
Restarting SNMP Monitoring on Fabric Nodes	595
Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node	596
Adding a Third-Party SNMP V3 Manager on a Fabric Node	596
Deleting a Third-Party SNMP Manager from a Fabric Node	597
Creating a System Snapshot	598
Deleting a System Snapshot	600
Restoring the System to a Snapshot	600
Chapter 62 Managing Databases	603
Backing Up and Restoring the Database	604
Backing up a Database	604
Restoring a Database	605
Backing Up the Database	605
Backing Up the Database to a Local Directory	606
Backing Up the Database to a Remote Host	608
Restoring a Database in the User Interface	610
Restoring a Local Database	610
Restoring the Database from a Remote File	611
Viewing Database Backup Files	613
Changing Views	613
Viewing Database Details	613

	Manage Database Commands	614
	Deleting Database Backup Files	614
	Viewing Job Recurrence	615
Chapter 63	Manage Licenses	617
	Generating and Uploading the Junos Space License Key File	617
	Generating the License Key File	618
	Uploading the License Key File Contents	618
	Viewing Licenses	619
	Viewing License Details	619
Chapter 64	Manage Applications	621
	Application Management Overview	621
	Managing Junos Space Applications	622
	Installing or Upgrading an Application	623
	Viewing Detailed Application Information	623
	Performing Manage Application Actions	624
	Modifying Application Settings	624
	Modifying Network Application Platform Settings	626
	Configuring Password Settings	628
	Managing Services	631
	Configuring Network Activate Application Settings	634
	Adding a Junos Space Application	635
	Junos Space Software Upgrade Overview	637
	Upgrading a Junos Space Application	638
	Upgrading Junos Space Software Overview	639
	Junos Space 13.1 Release Highlights	640
	Before You Begin	640
	Upgrading Junos Space Release to Release 13.1 and Later Versions	641
	Upgrading Junos Space Network Management Platform	641
	Uninstalling a Junos Space Application	646
Chapter 65	Troubleshoot Space	647
	System Status Log File Overview	647
	System Status Log File	647
	Customizing Status Log File Content	648
	Downloading System Log Files for a Junos Space Appliance	648
	Customizing Log Files To Download	648
	Customizing Node System Status Log Checking	649
	Customizing Node Log Files To Download	650
	Downloading the Troubleshooting Log File from the UI	650
	Downloading the Troubleshooting Log File In Maintenance Mode	652
	Downloading Troubleshooting System Log Files Using the CLI	653
	Downloading a System Log File Using a USB Device	653
	Downloading System Log File Using SCP	654
Chapter 66	Manage Certificates	657
	Certificate Management Overview	657
	Workflow	657
	Loading a Custom Junos Space Server Certificate	659

	Loading a User Certificate	659
	Loading CA Certificates and CRLs	660
	Changing the Authentication Mode	661
	Invalid Certificates	662
	Installing Custom SSL Certificate on the Junos Space Server	662
	Changing the Default Junos Space Server SSL Certificate	663
	Installing an X.509 Junos Space Server Certificate	663
	Installing a PKCS #12 Format Junos Space Server Certificate	664
	Certificate Expiry	665
	Certificate Attributes	665
Chapter 67	Manage Authentication Servers	667
	Remote Authentication Overview	667
	Understanding Junos Space Authentication Modes	668
	Local Authentication	668
	Remote Authentication	668
	Remote-Local Authentication	669
	Managing Remote Authentication Servers	669
	Creating a Remote Authentication Server	670
	Modifying Authentication Settings	672
	Configuring a RADIUS Server for Authentication and Authorization	673
	Configuring TACACS+ for Authentication and Authorization	677
	Junos Space Log In Behavior with Remote Authentication Enabled	679
Chapter 68	Manage SMTP Servers	683
	Managing Platform SMTP Servers	683
	Adding a Platform SMTP Server	684
Chapter 69	Manage Tags	687
	Overview	687
	Managing Tags Overview	687
	Managing Tags	688
	Managing Tags	688
	Managing Hierarchical Tags	689
	Using the Tag Hierarchy Pane	690
	Using the Tabular View Pane	693
	Sharing a Tag	693
	Renaming Tags	694
	Deleting Tags	695
	Tagging an Object	695
	Viewing Tags	696
	Untagging Objects	697
	Filtering Inventory Using Tags	697
	Creating Tags	698
	Creating a Tag	698

Chapter 70	Manage Permission Labels	701
	Managing Permission Labels Overview	701
	Understanding Subobject-Level Access Control	704
	Working With Permission Labels	705
	Creating Permission Labels	706
	Assigning Permission Labels to Users	706
	Attaching Permission Labels to Objects	707
	Managing Subobjects	709
Chapter 71	Manage DMI Schemas	713
	Managing DMI Schemas Overview	714
	Updating a DMI Schema	716
	Creating a Compressed Tar File for Updating DMI Schema	719
	Setting a Default DMI Schema	722
	Troubleshooting DMI Schema Management	723
Chapter 72	Generate Key	725
	Key-based Authentication Overview	725
	Generating and Uploading Authentication Keys to Devices	726
	Generating Keys	726
	Uploading Keys to Devices for the First Time	726
	Upload Keys on Managed Devices that have Conflicting keys with Junos Space	728
	Verifying Device Key Status	729
Part 13	Systems of Record and Disaster Recovery	
Chapter 73	Systems of Record and Disaster Recovery	733
	Understanding Systems of Record in Junos Space	733
	Systems of Record	733
	Implications	734
	Understanding Disaster Recovery	734
	Overview	735
	Prerequisites	735
	Creating the DR Master Cluster	736
	1. Configuring the DR Master Cluster	737
	2. Starting the Backup for the DR Master Cluster	738
	3. Stopping the Backup	739
	Creating the DR Slave Cluster	739
	1. Configuring the DR Slave Cluster	740
	2. Starting to Pull the Backups From the DR Master	741
	3. Stopping Pulling the Backups from the DR Master	742
	4. Restoring	743
	Performing a Reverse Restore	744
Part 14	Index	
	Index	747

List of Figures

Part 1	Junos Space User Interface	
Chapter 2	Understanding the Junos Space User Interface	9
	Figure 1: Junos Space First Display	10
	Figure 2: Junos Space Banner	10
	Figure 3: Platform Dashboard	13
	Figure 4: Workspace Statistics Pages	15
	Figure 5: Sorting Tables	17
	Figure 6: Showing or Hiding Columns in Tables	17
	Figure 7: Typical Filter Submenu	18
	Figure 8: Search	18
	Figure 9: Page Information Bar	19
	Figure 10: Typical Submenu for a Date Column	30
Part 2	Devices	
Chapter 3	Device Management Overview	35
	Figure 11: Device Count by Platform Report	37
	Figure 12: Device Status Report	38
	Figure 13: Device Count by OS Report	39
	Figure 14: Device Management Page	42
	Figure 15: Resynchronization Process	48
Chapter 10	Discover Devices	131
	Figure 16: Modify SNMP Setting Dialog Box	135
	Figure 17: SNMP v3 Options	136
Chapter 13	Secure Console	157
	Figure 18: Validating the Server Key Fingerprint	158
Part 3	Device Templates	
Chapter 16	Overview	177
	Figure 19: Workflow for Device Template Definition and Template Creation	181
Chapter 17	Template Definitions	183
	Figure 20: Template Definition Workflow	188
	Figure 21: CSV File for SNMP Contact	200
Part 4	CLI Configlets	
Chapter 20	Managing CLI Configlets	243
	Figure 22: CLI Configlets Statistics	247

Chapter 22	Managing Configuration Views	261
	Figure 23: Configuration Views Chart	264
Part 11	Audit Logs	
Chapter 57	View	531
	Figure 24: Formatting the Local Times Column in Microsoft Excel	537
Part 12	Administration	
Chapter 61	Fabric	551
	Figure 25: Fabric Nodes	552
	Figure 26: Fabric with One Node	554
	Figure 27: Fabric with Two Nodes	554
	Figure 28: Fabric with Three Nodes	555
	Figure 29: Overall System Condition Gauge	569
	Figure 30: Fabric Load History Chart	570
	Figure 31: Disk Usage Threshold Is Normal	575
	Figure 32: Trap Details When Disk Usage Normal	575
	Figure 33: Disk Usage Threshold Exceeds Configured Threshold	575
	Figure 34: Trap Details When Disk Usage Exceeds Configured Threshold	575
	Figure 35: CPU Load Average Threshold Is Normal	578
	Figure 36: Trap Details When CPU Load Average Threshold Is Normal	578
	Figure 37: CPU Load Average Threshold – Upper Limit Exceeded	578
	Figure 38: Trap Details When CPU Load 5 Minute Average Exceeds Threshold	578
	Figure 39: NMA Is Up	580
	Figure 40: Trap Details When NMA Is Up	580
	Figure 41: NMA is Down	580
	Figure 42: Trap Details When NMA is Down	580
	Figure 43: WebProxy Is Up	581
	Figure 44: Trap Details When WebProxy Is Up	581
	Figure 45: WebProxy Is Down	581
	Figure 46: Trap Details When WebProxy Is Down	581
	Figure 47: JBoss Is Up	582
	Figure 48: Trap Details When JBoss Is Up	582
	Figure 49: JBoss Is Down	582
	Figure 50: Trap Details When JBoss Is Down	582
	Figure 51: Mysql Is Up	583
	Figure 52: Trap Details When Mysql Is Up	583
	Figure 53: Mysql Is Down	583
	Figure 54: Trap Details When Mysql Is Down	583
	Figure 55: Postgresql Is Up	584
	Figure 56: Trap Details When Postgresql Is Up	584
	Figure 57: Postgresql Is Down	584
	Figure 58: Trap Details When Postgresql Is Down	584
	Figure 59: Swap Memory Usage Is Normal	585
	Figure 60: Trap Details When Swap Memory Is Normal	585
	Figure 61: Swap Memory Usage Threshold Exceeds Upper Limit	585

	Figure 62: Trap Details When Swap Memory Usage Exceeds Upper Limit	585
	Figure 63: CPU Fan Speed Normal	588
	Figure 64: Trap Details When CPU Fan Speed Is Normal	588
	Figure 65: CPU Fan Speed Is Below the Configured Threshold	588
	Figure 66: Trap Details When CPU Fan Speed Is Below the Configured Threshold	588
	Figure 67: CPU Voltage Normal	590
	Figure 68: Trap Details When CPU Voltage Is Normal	590
	Figure 69: CPU Voltage Is Lower Than Configured Threshold	590
	Figure 70: Trap Details When CPU Voltage Is Lower Than Configured Threshold	590
	Figure 71: CPU Temperature Normal	591
	Figure 72: Trap Details When CPU Temperature Is Normal	591
	Figure 73: CPU Temperature Exceeds The Configured Threshold	591
	Figure 74: Trap Details When CPU Temperature Exceeds The Configured Threshold	591
	Figure 75: Trap Details Junos Space Node Is Down	593
	Figure 76: Trap Details Junos Space Node Is Up	593
	Figure 77: Trap Details Junos Space Node Is Deleted	593
	Figure 78: 6412-monitoring-nodes-netmon-node-list	595
Chapter 65	Troubleshoot Space	647
	Figure 79: Maintenance Mode Page	652

List of Tables

	About the Documentation	xxxi
	Table 1: Notice Icons	xxxii
	Table 2: Text and Syntax Conventions	xxxii
Part 1	Junos Space User Interface	
Chapter 2	Understanding the Junos Space User Interface	9
	Table 3: Global Action Icons	10
	Table 4: Task Group (Workspace) Names	11
	Table 5: Gadget Mouse-Over and Selection Operations	14
	Table 6: Inventory Page Banner Icon Buttons	16
	Table 7: Table Paging and Refreshing Controls	20
	Table 8: Searchable Objects	21
	Table 9: Supported Query Expressions in the Search Field	25
	Table 10: Filter-enabled Tables and Columns	28
Part 2	Devices	
Chapter 3	Device Management Overview	35
	Table 11: Fields in the Device Management Table	43
	Table 12: Device Connection Status Icon	44
Chapter 4	Device Configuration	51
	Table 13: Selected Devices Columns	58
	Table 14: Configuration Change Log	65
	Table 15: Resolving Out-of-Band Changes	66
	Table 16: View Configuration Change Log Table	67
	Table 17: View Assigned Shared Objects Table	68
Chapter 5	Device Inventory	73
	Table 18: Physical Interfaces Columns	76
	Table 19: Logical Interfaces Columns	79
	Table 20: License Usage Summary Fields	82
	Table 21: License Feature or SKU Fields	83
	Table 22: Additional Fields in CSV Files	83
	Table 23: Software Inventory Fields	85
Chapter 8	Device Monitoring	119
	Table 24: Information Displayed in the Alarms List	121
Chapter 11	Deployed Devices	139
	Table 25: Icons to View or Download Management CLI Commands	140

	Table 26: Icons in the Rapid Deployment dialog box	148
	Table 27: Fields Manually Entered in the Rapid Deployment Dialog Box	148
Chapter 12	Unmanaged Devices	153
	Table 28: SNMP V3 Configuration Parameters	154
	Table 29: Sample CSV for Importing Unmanaged Devices	154
Part 3	Device Templates	
Chapter 17	Template Definitions	183
	Table 30: Data Types and Tabs	192
	Table 31: Data Types and Validation Parameters	193
	Table 32: CSV File for Interfaces	201
Chapter 18	Templates	209
	Table 33: Device Template State Icon Indicators	210
	Table 34: Descriptive Information	210
	Table 35: Review Changes Page	216
	Table 36: View Deployment Table	217
Part 4	CLI Configlets	
Chapter 19	CLI Configlets Overview	233
	Table 37: Parameters for a Configlet	235
	Table 38: Configlets User Roles Permissions	237
Chapter 20	Managing CLI Configlets	243
	Table 39: Configlet Details	243
	Table 40: Parameters Page	244
Part 5	Images and Scripts	
Chapter 24	Overview	269
	Table 41: Device Images and Scripts User Roles	270
Chapter 25	Device Images	273
	Table 42: Manage Images Page	273
Chapter 26	Scripts	275
	Table 43: Scripts Page Fields Description	276
Chapter 29	Configuration: Device Images	283
	Table 44: Stage Image On Devices Dialog Box Fields Descriptions	285
	Table 45: Routing Platforms and Software Releases Supporting ISSU	287
	Table 46: Common Deployment Options Description	291
	Table 47: Conventional Deployment Options Description	291
	Table 48: ISSU Deployment Options Description	292
	Table 49: Advanced Deployment Options Description	292
	Table 50: Select Devices Table Field Descriptions	292
	Table 51: Validation Results Page Field Descriptions	295
Chapter 30	Configuration: Scripts	297
	Table 52: View Execution Result Page Fields Description	312

Chapter 31	Configuration: Operations	315
	Table 53: Create Operation Dialog Box Icon Descriptions	317
Chapter 32	Configuration: Script Bundles	325
	Table 54: Create Script Bundle Dialog Box Icon Descriptions	326
	Table 55: Modify Script Bundle Dialog Box Icon Descriptions	327
Chapter 33	Administration: Scripts	335
	Table 56: Script Details Dialog Box Fields	335
	Table 57: Script Verification Results Page Fields	336
Part 6	Reports and Report Definitions	
Chapter 37	Report Definitions	349
	Table 58: Audit Trail Report Definition Attributes	350
	Table 59: Device Inventory Report Definition Attributes	350
	Table 60: Device License Inventory Report Definition Attributes	351
	Table 61: Device Logical Interface Inventory Report Definition Attributes	352
	Table 62: Device Physical Interface Inventory Report Definition Attributes	353
	Table 63: Device Software Inventory Report Definition Attributes	353
	Table 64: Job Inventory Report Definition Attributes	354
Part 7	Network Monitoring	
Chapter 40	Monitoring Devices and Assets	371
	Table 65: Alarms Table	376
	Table 66: Notifications Table	376
	Table 67: Node Status Table	377
	Table 68: Resource Graphs Table	377
	Table 69: Alarm Details	379
Chapter 41	Working With Events, Alarms, and Notifications	387
	Table 70: Information Displayed in the Alarms List	393
Part 9	Jobs	
Chapter 49	Overview	461
	Table 71: Junos Space Job Types Per Application	462
Chapter 50	Manage Jobs	465
	Table 72: Job Icon Status Indicators	466
	Table 73: Job Details and Columns in the Manage Jobs Table	467
Part 10	Users	
Chapter 52	Manage Roles	479
	Table 74: Predefined Roles for the Junos Space Network Management Platform	482
	Table 75: Predefined Roles for Network Activate Application	493
	Table 76: Predefined Roles for Service Insight Application	495
	Table 77: Predefined Roles for Service Now Application	497

	Table 78: Predefined Roles for Ethernet Design Application	501
Chapter 54	Manage Users	509
	Table 79: User Detail Summary Page	519
Part 11	Audit Logs	
Chapter 57	View	531
	Table 80: Detailed Audit Logs Information and View Audit Log Table Columns	533
	Table 81: Audit Log Table Details for Recurring and Non-recurring Jobs	533
Part 12	Administration	
Chapter 60	Overview	547
	Table 82: Junos Space Administrators	547
Chapter 61	Fabric	551
	Table 83: Fields for the Fabric Monitoring Inventory Page	558
	Table 84: Logical Component Monitoring	571
	Table 85: SNMP Configuration Parameters: Monitoring Disk Usage	574
	Table 86: SNMP Configuration Parameters: Monitoring the CPU Load Average	577
	Table 87: SNMP Configuration Parameters: Monitoring Processes	580
	Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware	586
Chapter 62	Managing Databases	603
	Table 89: Backup Schedule Units and Increments	607
	Table 90: Fields in the Manage Databases Table	613
Chapter 63	Manage Licenses	617
	Table 91: Licenses Details	619
Chapter 64	Manage Applications	621
	Table 92: Application Information	623
	Table 93: Junos Space Network Management Platform Application Settings . .	626
	Table 94: Password Constraint Parameters	629
	Table 95: Starting, Stopping, and Restarting Network Monitoring	632
	Table 96: Network Activate Application Settings	634
Chapter 65	Troubleshoot Space	647
	Table 97: Log Files included in the troubleshoot File	648
	Table 98: Data and Log Files in troubleshoot.zip File	651
Chapter 66	Manage Certificates	657
	Table 99: Certificate Attributes	665
Chapter 67	Manage Authentication Servers	667
	Table 100: Remote Authentication Server Settings	671
	Table 101: TACACS+ Remote Authentication Server Settings	677
Chapter 69	Manage Tags	687
	Table 102: Tag Information	689

Chapter 71	Manage DMI Schemas	713
	Table 103: Sample URLs for the Repository	720

About the Documentation

- Documentation and Release Notes on page xxxi
- Documentation Conventions on page xxxi
- Documentation Feedback on page xxxiii
- Requesting Technical Support on page xxxiv

Documentation and Release Notes

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

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

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

Documentation Conventions

Table 1 on page xxxii defines notice icons used in this guide.

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

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

Documentation Feedback

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

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Junos Space User Interface

- [Getting Started on page 3](#)
- [Understanding the Junos Space User Interface on page 9](#)

CHAPTER 1

Getting Started

- Logging In to Junos Space on page 3
- Changing User Passwords on page 4
- Using the Getting Started Assistants on page 5
- Accessing Help on page 6
- Logging Out on page 6

Logging In to Junos Space

You connect to Junos[®] Space from your Web browser. Internet Explorer versions 8.0 and 9.0, and latest stable versions of Mozilla Firefox and Google Chrome Web browsers are supported.



WARNING: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space in a browser tab or window, make sure that the tab or window was not previously used to surf a non-https website. Best practice is to close your browser and relaunch it before logging in to Junos Space.



NOTE: Before you can log in to the system, your browser must have the Adobe Flash Version 10 or later plug-in installed.



NOTE: If you are using Internet Explorer to connect to Junos Space, install the Google Chrome Frame plug-in for the Topology Discovery feature to work properly.

To access and log in to Junos Space:

1. In the address field of your browser window, type
https://<IP Address>/mainui/
where <IP Address> is the Web IP address for Web access to Junos Space.
2. Press Enter or click **Search**.

The system login screen appears.

3. Type your username and password. The default username is **super**; the password is **juniper123**. For information about how to change your username, consult your system administrator.
4. (Optional) Perform remote authentication with Challenge-Response configured on a server.

Provide valid responses for the challenge questions you are asked to log in successfully.

5. Click **Log In**.

The Junos Space Network Management Platform dashboard appears.



NOTE: By default, Junos Space Network Management Platform authenticates a user using its username and password. However, you can use certificates to authenticate and authorize sessions among various servers and users. To configure certificate-based authentication, see [“Certificate Management Overview” on page 657](#).

Related Documentation

- [Logging Out of Junos Space on page 6](#)
- [Changing Your Password on Junos Space on page 4](#)
- [Junos Space User Interface Overview on page 9](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Changing User Passwords

Users who are logged in to Junos Space Network Management Platform can change their account passwords by using the User Preferences icon on the Junos Space application banner. No particular Junos Space role is required for users to change their passwords.

Beginning with Junos Space Network Management Platform Release 12.1, Junos Space has implemented a default standard for passwords that is compliant with industry standards for security.



NOTE: Upgrading to Junos Space Platform 12.1 or later causes the default standard to take effect immediately. All local users will get password expiration messages the first time they log in after the update.



NOTE: If you do not have a local password set, you will not be able to set or change it.



NOTE: Using User Preferences to change your password only works for local passwords. The change does not affect any passwords that an administrator might have configured for you on a remote authentication server.

To change your user password:

1. Click the User Preferences icon on the upper right, in the Junos Space application banner.

The User Preferences – Change Password dialog box appears.

2. Type your old password.
3. Display the rules for password creation by mousing over the information icon (small blue [i]) next to the password field.

Type your new password.

4. Retype your password to confirm it.
5. Click **OK**.

You are logged out of the system. You have to log in again using your new password. Other sessions for the same user are unaffected until the next login.

Related Documentation

- [Creating User Accounts on page 509](#)
- [Logging In to Junos Space on page 3](#)
- [Configuring Password Settings for Junos Space Network Management Platform on page 628](#)

Using the Getting Started Assistants

The Getting Started assistants display steps and help on how to complete common tasks. Getting Started is a section in the sidebar that appears when you log in to the system if the **Show Getting Started on Startup** check box at the bottom of the section is selected. If the sidebar is not shown, you can display it by selecting the Help icon in the Junos Space header.

The Getting Started topics are context-sensitive per application. Getting Started displays all the steps in a task. From a step in a task, you can jump to that point in the user interface to actually complete it.

Some applications implement the Getting Started assistants; others do not.

To use a Getting Started assistant:

1. Select an application in the task tree.
2. If the sidebar is not already displayed, select the **Help** icon at the right side of the Junos Space header. (Mouse over the icons to see their descriptions.)
The sidebar appears.

3. In the sidebar, expand **Getting Started**.

A main Getting Started topic link appears in the sidebar.

4. Select a main topic.

For example, in the Network Management Platform application, click **Increase Space Capacity** link. A list of required steps appears in the sidebar. Each step contains a task link and a link to the Help.

5. Perform a specific step by clicking the link.

You jump to that point in the user interface. The assistant remains visible in the sidebar to aid navigation to subsequent tasks.

6. Access Help for a specific step by clicking the Help icon next to that step.

**Related
Documentation**

- [Accessing Help on Junos Space on page 6](#)

Accessing Help

Junos Space provides complete documentation in a Help system that is context-sensitive per workspace. The Help system provides information about each element in the system, including workspaces, dashboards, tasks, inventory pages, and actions. The Help system also provides frequently asked questions (FAQs) and the entire system documentation. Help topics appear as links in the sidebar.

To access online Help:

1. Click the workspace within which you want to work.
2. Click the Help icon.

The sidebar appears, if it is not already displayed, with the Help section open listing specific topics for that workspace and tasks.

3. Click a topic link to view its contents.

The Help topic appears in a separate window.

4. Click the >> button at the top right of the sidebar to hide it.

**Related
Documentation**

- [Using the Getting Started Assistants on page 5](#)
- [Junos Space User Interface Overview on page 9](#)

Logging Out

When you complete your administrative tasks in the Junos Space user interface, log out to prevent unauthorized users from intruding.

To log out of the system:

1. Click the **Log Out** icon in the Junos Space application banner.

The logout page appears. A user who is idle and has not performed any action, such as keystrokes or mouse-clicks, is automatically logged out of Junos Space to the Logout page. This setting conserves server resources and protects the system from unauthorized access. The default setting is 5 minutes. You can change the setting on the Applications inventory page. Select **Administration > Applications > Network Management Platform > Modify Application Settings > User > Automatic logout after inactivity (minutes)**.

To log in to the system again, click the **Click here to log in again** link on the logout page.

**Related
Documentation**

- [Logging In to Junos Space on page 3](#)
- [Changing Your Password on Junos Space on page 4](#)
- [Modifying Junos Space Application Settings on page 624](#)
- [Junos Space User Interface Overview on page 9](#)

CHAPTER 2

Understanding the Junos Space User Interface

- [Junos Space User Interface Overview on page 9](#)
- [Global Search on page 20](#)
- [Navigating the Junos Space User Interface on page 26](#)
- [Filtering Inventory Pages on page 27](#)

Junos Space User Interface Overview

The Junos Space user interface is designed to look and behave in a familiar way for most users. To familiarize yourself with it quickly, try the example in [“Navigating the Junos Space User Interface” on page 26](#). It will direct you back to this topic for any less-than-obvious details.

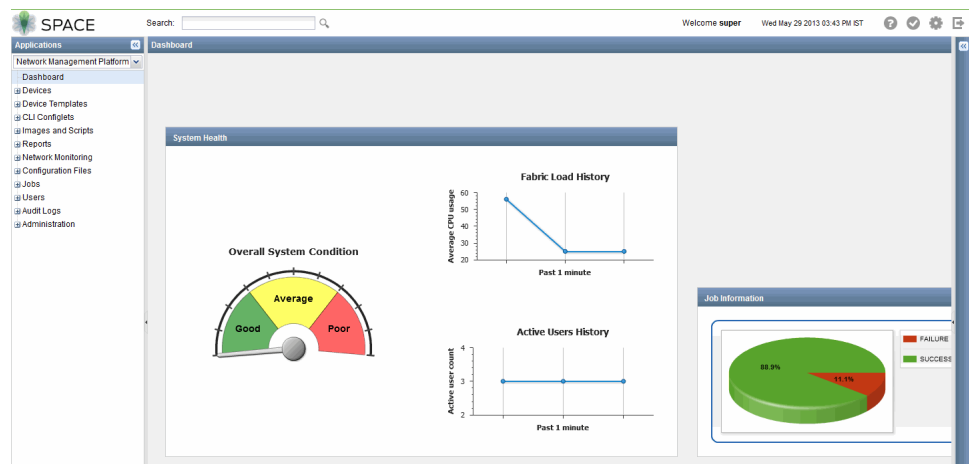
Multiple users can have concurrent access to the user interface via Web browsers. All users have access to the same current information in the same system wide database. Access to tasks and objects is controlled by permissions assigned to each user.

The examples shown here are from the Junos Space Network Management Platform user interface. Other applications may have design variations.

The Main Display

When you have logged in to Junos Space, the first display you see is shown in [Figure 1 on page 10](#).

Figure 1: Junos Space First Display



This display has three main parts: a task tree on the left, which is always available; a main window on the right, whose content changes as you select items from the task tree; and a banner across the top, which offers the date and time, global search, and several icon buttons for frequently used actions. These parts are described in the following sections.

- [Banner on page 10](#)
- [Task Tree on page 11](#)
- [Main Window on page 12](#)

Banner

The banner displays the date and server time in the active time zone, global search, and the global actions icons.

Figure 2: Junos Space Banner



This banner is always present. [Table 3 on page 10](#) describes the global action icons on the right side of the banner.

Table 3: Global Action Icons

Global Action Icon	Description
	Displays the application Help. To access workspace context-sensitive Help, click the Help icon after navigating to that workspace. See “Accessing Help on Junos Space” on page 6 .
	Displays the My Jobs dialog box from which you can view the progress and status of current managed jobs. See “Viewing Your Jobs” on page 465 .
	Displays the User Preferences dialog box from which you can change user preferences, such as the password. See “Changing Your Password on Junos Space” on page 4 .
	Logs you out of the system. See “Logging Out of Junos Space” on page 6 .

For more information about global search, see [“Global Search” on page 20](#).

Task Tree

The task tree on the left side of the display is always present and is the navigation center for Junos Space. As shown in [Figure 1 on page 10](#), when you first log in, the box at the top of the tree beneath the Applications banner displays Network Management Platform by default. You can drop this list down to see all the other Junos Space applications available on your system. (You can install other applications using the Manage Applications task group, as described in the [“Application Management Overview” on page 621](#).)

You can collapse the task tree to the left by clicking the Double Left arrows in its header, and re-expand it by clicking the Double Right arrows.

Below the application name is the word Dashboard, selected by default. It indicates that what you see in the right-hand window is the dashboard for the current application, in this case for the Platform. The dashboard shows several measures of overall system health.

Below the Dashboard item in the tree is a list of the task groups available in the current application. This list forms the top level of the task tree. If you select a different application from the Application box, you will see the task group list change. This topic describes the task groups for the Platform; for the task groups in other applications, see their respective documentation.

The task groups in the Platform are described at a high level in [Table 4 on page 11](#).

Table 4: Task Group (Workspace) Names

Task Group Name	Function
Devices	Manage devices, including adding, discovering, importing, and updating them. See “Device Management Overview” on page 35 .
Device Templates	Create configuration definitions and templates used to deploy configuration changes on multiple Juniper Networks devices. See “Device Templates Overview” on page 178 .
Device Images and Scripts	<p>Download a device image from the Juniper Networks Software download site to your local file system, upload it into Junos Space, and deploy it on one or more devices simultaneously. See “Device Images Overview” on page 273.</p> <p>Use Junos OS scripts (configuration and diagnostic automation tools) to deploy, verify, enable, disable, remove, and execute scripts deployed to devices.</p>
Network Monitoring	Assess the performance of your network, not only at a point in time, but also over a period of time. See “Network Monitoring Workspace Overview” on page 365 .

Table 4: Task Group (Workspace) Names (*continued*)

Task Group Name	Function
Config Files	Maintain copies of device running, candidate, and backup configuration files, providing for device configuration recovery and maintaining consistency across multiple devices. See “Managing Configuration Files Overview” on page 444 .
Job Management	Monitor the progress of ongoing jobs. See “Jobs Overview” on page 461 .
Users	Add, manage, and delete users. See “Configuring Users to Manage Objects in Junos Space Overview” on page 480 .
Audit Logs	View and filter system audit logs, including those for user login and logout, tracking device management tasks, and displaying services that were provisioned on devices. See “Junos Space Audit Logs Overview” on page 531 .
Administration	Add network nodes, back up your database, manage licenses and applications, or troubleshoot. See “Adding a Node to an Existing Junos Space Fabric” on page 556 , “Backing Up and Restoring the Database Overview” on page 604 , “Downloading the Troubleshooting Log File from the UI” on page 650 , “Downloading the Troubleshooting Log File In Maintenance Mode” on page 652 , “Application Management Overview” on page 621 , “Viewing Tags for a Managed Object” on page 696 .

You can expand any of these task groups by clicking the expansion symbol to the left of its name. When you do so, the next level of the task tree for that task group opens. Some items at this second level may also be expandable subgroups. The tree does not go deeper than three levels.

You can expand as many task groups as you like: previously expanded ones remain open until you collapse them. The design of the task tree enables you to jump from area to area within an application with the minimum number of selections.

Main Window

When you log into Junos Space, the main window shows the Platform application dashboard.

When you select a task group name (as opposed to expanding it), the main window changes and displays graphical statistics for that task group. Task groups are also referred to as workspaces, so this display is called Workspace Statistics. It is similar in functionality to the overall system dashboard, but it pertains only to that task group.

Selecting the name of a subtask whose name begins with “Manage” causes the main window to display an inventory of the objects managed in table format.

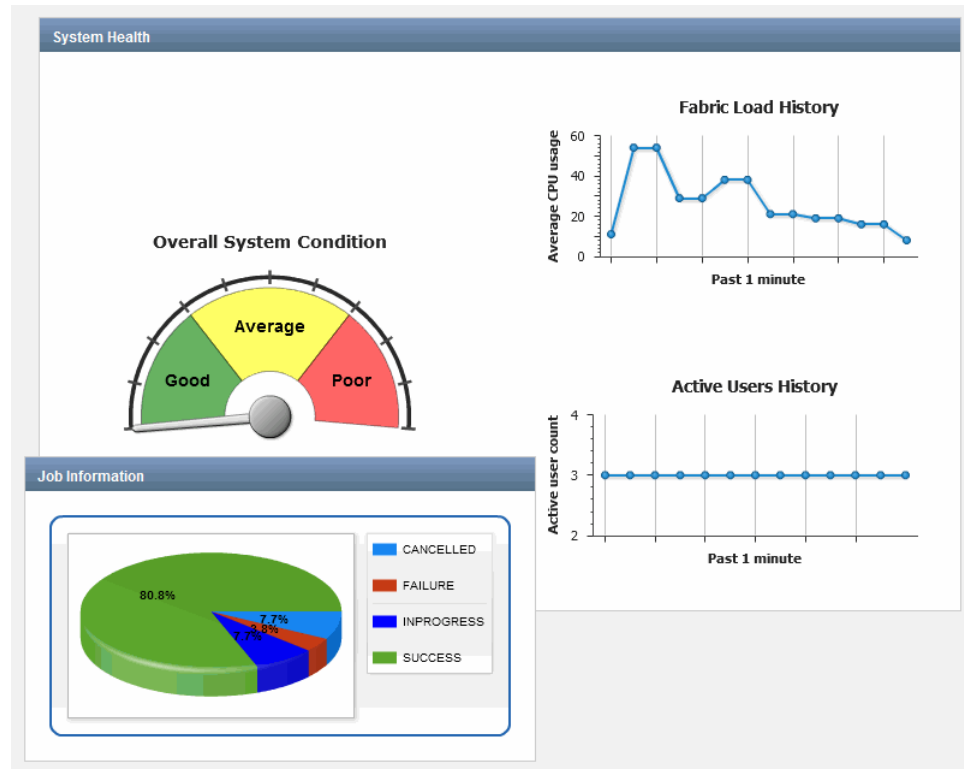
Each of these tools is discussed in a later section of this topic.

Application Dashboard

When you select an application in the box above the task tree, a dashboard displays graphical data about devices, jobs, users, administration, and so on.

The dashboard provides a snapshot of the current status of objects managed and operations performed within a Junos Space application. The Platform dashboard, displays the system health of your network and the percentage of jobs run successfully and in progress.

Figure 3: Platform Dashboard



The following sections describe the parts of the Platform Dashboard.

Dashboard Gadgets

The Platform dashboard contains gadgets (graphs and charts) that display statistics that provide a quick view of system health. They include a gauge for overall system condition and graphs that display the fabric load and active users history. For an explanation of the data shown in these gadgets, see [“Overall System Condition and Fabric Load History Overview”](#) on page 568.

You can move and resize gadgets. All dashboard gadgets are visible for all users and are updated in real time. To print or save a graph or chart, right-click it to bring up a menu.

Select (single-click) a gadget or gadget elements to see more detailed information. Typically, selecting a gadget element takes you either to the statistics page of the

associated task group, or to an inventory page. Some gadgets let you filter information by selecting a specific segment or bar from a chart, or a specific line of a table. For example, if you select the red segment on the Job Information gadget, you navigate to the Job Management > Manage Jobs inventory page, which in this case displays only failed tasks.

Return to the dashboard by selecting Dashboard in the task tree.



NOTE: If you do not have user privileges to view certain application data, you cannot view more detailed information if you select a gadget.

Table 5 on page 14 describes the mouse-over and selection (single-click) operations you can perform on dashboard gadgets.

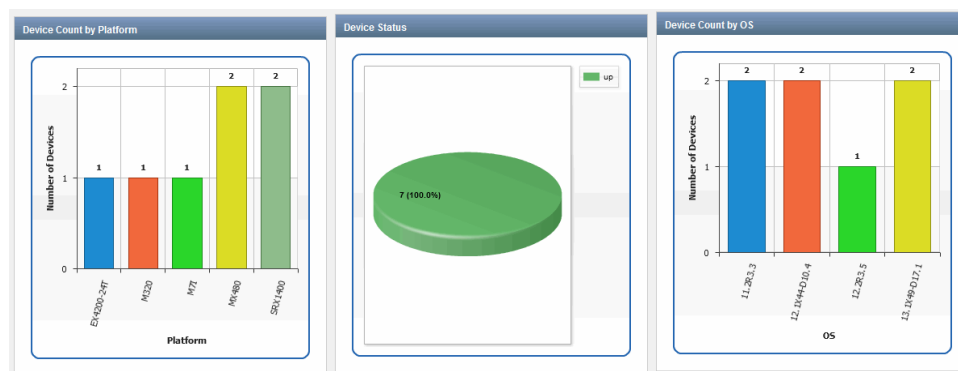
Table 5: Gadget Mouse-Over and Selection Operations

Gadget	Mouse-Over Information	Double-Click Navigation
Overall System Condition gauge	–	Select the indicator needle to display the Administration > Manage Fabric page. See “Overall System Condition and Fabric Load History Overview” on page 568.
Fabric Load History graph	Mouse over a graph data point to view the CPU usage (average usage percentage)	Select a graph data point to display the Administration > Manage Fabric page. See “Viewing Nodes in the Fabric” on page 557.
Active Users History graph	Mouse over a graph data point to view the active users history (total count)	Select the graph data point to display the Users statistics page, filtered by active users. See “Viewing User Statistics” on page 524.
Job information pie chart	Mouse over the pie chart to view the percentage of jobs that have been successful.	Select a segment of the pie chart to display the Job Management > Manage Jobs inventory page, filtered by that segment. To see the list unfiltered, select the red X beside the filter criterion, above the column headings on the left side. See “Viewing Scheduled Jobs” on page 466.

Task Group (Workspace) Statistics

When you select the name of a task group (workspace) in the task tree, Junos Space displays high-level statistics representing the status of managed objects in that task group.

Figure 4: Workspace Statistics Pages



To print or save the statistics, right-click the graphic (bar chart or pie chart).

You can move charts and graphs on the screen or resize them.

If a chart has more data points than can be viewed clearly simultaneously, a scroll bar appears at the bottom or side of the chart.

If you click a bar or pie-chart segment, you navigate to the corresponding inventory page, filtered according to the bar or segment you selected. For example, if you click the MX240 devices bar in the Device Count by Platform bar chart, you navigate to the Platform > Devices > Manage Devices inventory page, which in this case displays all the MX240 devices on the network that are discovered and managed by Junos Space.

If you click the slice in the Device Status pie chart that represents the number of devices that are down, you navigate to the Manage Devices inventory page that displays all the devices on the network that are down.

Inventory Page

Throughout the Junos Space user interface, you navigate to an inventory page by selecting an application, expanding an application task group, then selecting a management task, such as Manage Devices, Manage Users, or Manage Jobs. For example, to view the Manage Devices inventory page, select Platform > Devices > Manage Devices.

On the inventory pages, managed objects are displayed in tables. The columns shown vary depending on which Junos Space applications you have installed.

Each managed object stored in the Junos Space database includes specific data. For example, devices are stored in the database according to device name, interfaces, OS version, platform, IP address, connection, managed status, and several other items of information.

Inventory pages enable you to view and manipulate managed objects individually or collectively. Managed objects include devices, logs, users, jobs, clients, software, licenses, and so forth. You can browse, zoom, filter, tag, and sort objects.

You can manipulate objects in tables by changing the width of columns, sorting columns, and hiding columns.

Select an object or objects by selecting the check box to the left of each object. You can select one, several, or all objects and perform actions on them using right-click actions or items on the Actions menu on the right side of the inventory page banner. Selecting the box to the left in the first column of the column head row selects or deselects all items.



NOTE: The function and implementation of individual inventory pages depend on the Junos Space application design.

Banner Icon Buttons

Depending on the nature of the inventory page, its banner may contain any of the icons shown in [Table 6 on page 16](#). Mouse over an icon to see its name.

Table 6: Inventory Page Banner Icon Buttons

Symbol	Name	Function
	Tag	Displays or hides a left-side tag menu that allows you to filter inventory page contents according to tags. See "Filtering the Inventory by Using Tags" on page 697 .
	Display Quick View	Displays or hides a small window summarizing data about the selected object.
	Create <i>Object</i>	Displays a window in which you can create an instance of this type of object.
	Show <i>Object</i> Details	Displays a window containing full details about the selected object: for example, all the permissions of a user.
	Modify <i>Object</i>	Displays a window allowing you to edit the selected object.
	Delete <i>Object</i>	Deletes the selected object.

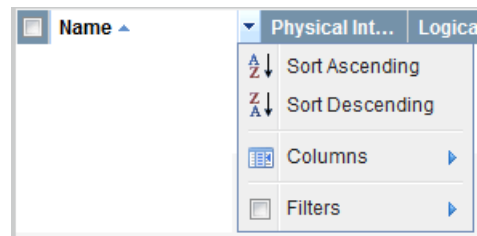
Return to the inventory page by closing the window in which you are currently in, if possible, or by selecting within the breadcrumbs at the top of the page.

Sorted-by Indicator

The Sorted-by indicator is a small arrowhead next to a column name. It displays how the objects are sorted in a column. After you have sorted a column, the column name is highlighted and the indicator appears.

You can sort inventory data using the Sort Ascending and Sort Descending commands in the column header drop-down menu. Click the down arrow on a table header to view the sort menu. In [Figure 5 on page 17](#), the device inventory is sorted by the Name column.

Figure 5: Sorting Tables

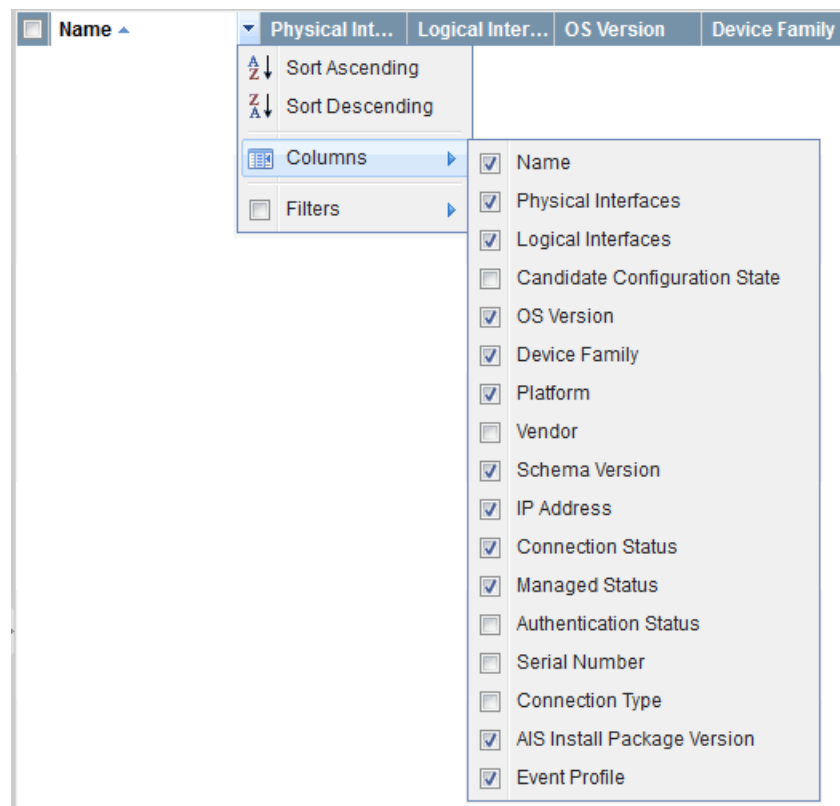


Some columns do not support sorting.

Show or Hide Columns

Hide table columns by deselecting the column name on the Columns Cascading menu, as shown in [Figure 6 on page 17](#). It is available in any column. Only selected column names appear in the inventory table.

Figure 6: Showing or Hiding Columns in Tables



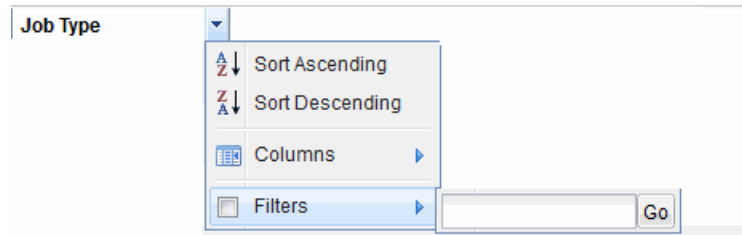
Filter Submenus

The Filter submenus let you temporarily hide all the entries in the table that do not match the criteria that you are interested in. These features let you quickly find and evaluate the table entries of interest. For details, see [“Filtering Inventory Pages” on page 27](#).

To filter tables on various criteria, right-click the column header and use the Filter submenu. The choices available depend on the nature of the selected column.

Whenever you filter a table, the application displays the filter criteria, including the columns being filtered, above the table. The inventory table also displays a red X to the left of the filter criteria. You can clear the filter and restore the table to its original view by clicking the red X.

Figure 7: Typical Filter Submenu

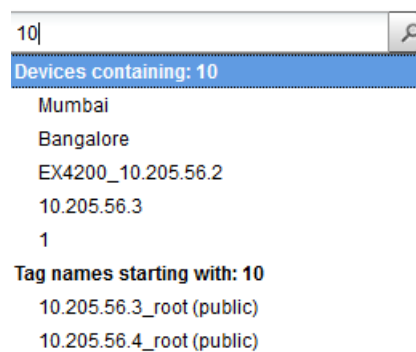


Search Field

Use the Search text field on the right of the inventory page banner to look for specific objects to display on the inventory landing page. To find objects (within any columns) on this page, enter the search criteria in the Search field. This field supports the same search syntax as the global search field (see [“Global Search” on page 20](#)). For example, enter “os:junos AND down” to find devices that are down on the devices inventory landing page. This feature is more powerful than the column filter because it allows you to use Boolean expressions.

Clicking the magnifying glass at the right in the search field displays a list of inventory objects. When you select a search option from the list, inventory items specific to that search option only are displayed on the page.

Figure 8: Search



You can create tags to categorize objects. For more information about tagging objects to select similar objects, see [“Tagging an Object” on page 695](#).

To display all the inventory objects on the page again, clear the contents of the Search box and press Enter.



NOTE: You must append "*" if you want to search using partial keywords. Otherwise, the search returns 0 (zero) matches or hits.

Actions Menu

You can perform actions on one or more selected items on an inventory page by using the Actions menu at the right side of the banner, or by right-clicking the items. To use the Actions menu, select one or more objects, select the Actions menu, and select an action or subgroup of actions. (A subgroup has an arrowhead next to its name.) For example, to view the physical interfaces of a device, select that device on the Manage Devices inventory page, open the Actions menu, expand the Device Inventory subgroup, and select View Physical Inventory.

You can also select one or more items on the inventory page, then right-click. The right-click menu appears, providing the same functionality as the Actions menu.



NOTE: If you are using Mozilla Firefox, the Advanced JavaScript Settings might disable the right-click menu.

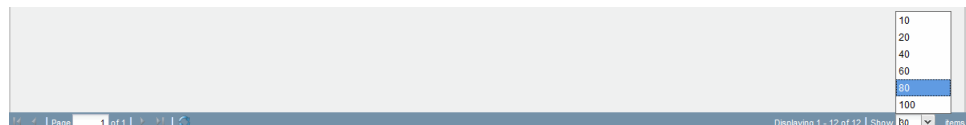
To ensure that you can use the right-click menu:

1. In Mozilla Firefox, select Tools > Options to display the Options dialog box.
2. In the Options dialog box, click the Content tab.
3. Click Advanced to display the Advanced JavaScript Settings dialog box.
4. Select the Disable or replace context menus option.
5. Click OK in the Advanced JavaScript Settings dialog box.
6. Click OK in the Options dialog box.

Paging Controls






Figure 9 on page 19 shows the paging controls that appear at the bottom of the inventory page. You can use these controls to browse the inventory when the inventory is too large to fit on one page.

Figure 9: Page Information Bar



The Page box lets you jump to a specific page of managed objects. Type the page number in the Page box and press Enter to jump to that page. The Show box enables you to customize the number of objects displayed per page. Table 7 on page 20 describes other table controls.

Table 7: Table Paging and Refreshing Controls

Page Control	Operation
	Advances to the next page of the table.
	Returns to the previous page of the table.
	Displays the last page of the table.
	Displays the first page of the table.
	Refreshes the table content.

- Related Documentation**
- [Device Management Overview on page 35](#)
 - [Tagging an Object on page 695](#)
 - [Filtering Inventory Pages on page 27](#)

Global Search

You can use the search feature at the top of the Junos Space user interface to quickly locate any object within Junos Space. Junos Space allows you to perform a full-text search operation for objects within the system.

The search results are displayed on the basis of how the Junos Space Network Management Platform objects are indexed. [Table 8 on page 21](#) lists the indexed objects on which you can perform a search operation by using the global search feature. The scope of search in Junos Space Release 13.1 is restricted to the objects in Junos Space Network Management Platform.

Table 8: Searchable Objects

Object Category	Indexed Fields (Objects)	Description
Device	name	Name of the device.
	deviceFamily	Device family, such as Junos OS, Junos ES, Junos EX, and so on
	platform	Hardware platform, such as MX80, EX4200-24T, and so on
	os	Junos OS version
	ip	Device management IP address
	connectionStatus	Device connection state—whether the device is up or down
	managedStatus	Device management status, such as “In Sync,” “Connecting,” “Sync Failed,” and so on
	serialNumber	Serial number
	ccState	Candidate Config State, such as “Created,” “Accepted,” or “Rejected.”
	vendor	Vendor
	authenticationStatus	Authentication status indicates how the device is connected to Space, such as “Credential Based,” “Key based,” or “Key Conflict.” Credential-based uses username and password for connection, whereas, key-based needs an RSA key for establishing a connection. The GUI displays key conflict when the keys on Junos Space and device are not the same.
	connectionType	Connection type

Table 8: Searchable Objects (*continued*)

Object Category	Indexed Fields (Objects)	Description
Physical interface	name	Name of the physical interface
	ip	Assigned IP address
	mac	MAC address
	operationStatus	Operational status—whether the operational status of the physical interface is up or down
	adminStatus	Administrative status—whether the administrative status of the physical interface is up or down
	linkLevelType	Link Level Type
	linkType	Link type of the physical interface, such as full-duplex or half-duplex
	speed	Link speed on the physical interface, which can be 800 Mbps, 1000 Mbps, and so on
	mtu	MTU of the physical interface. For example, 1514, 9192, Unlimited, and so on
	description	Description of the physical interface
Logical interface	name	Name of the logical interface
	ip	IP address
	encapsulation	Encapsulation on the logical interface, such as VLAN-VPLS
	vlanId	Assigned VLAN number
	description	Description of the logical interface

Table 8: Searchable Objects (*continued*)

Object Category	Indexed Fields (Objects)	Description
Device Physical Inventory	name	Module name of the hardware inventory
	version	Software release version
	modelName	Model number of the module
	model	Device family
	partNumber	Part number of the module
	serialNumber	Serial number of the module
	status	Status
	description	Description of the module
Software Inventory	model	The model of this device. Possible device families include J Series, M Series, MX Series, TX Series, SRX Series, EX Series, BXOS Series, and QFX Series.
	routingEngine	Routing engine
	name	Name of the installed software package.
	version	Version number of the installed software package.
	type	Type of the installed software package. Permitted values are operating-system, internal-package, and extension.
	major	Major portion of the version number. For example, in version 13.1R1.14, the major portion is 13.
	minor	Minor portion of the version number. For example, in version 13.1R1.14, the minor portion is 1.
	revisionNumber	The revision number of the package. For example, in version 13.1R1.14, the revision number is 1.14.
	description	Description of the installed software package.
Tags	name	List of tags assigned to an object

To search for objects using the global search feature:

1. In the **Search** field at the top of the Junos Space user interface, type the search criteria. Then press **Enter** or click the magnifying glass icon adjacent to the Search field.

All objects matching the search criteria appear on the search results page. The area on the left displays the search results with appropriate filters. The area on the right displays the search results with a short description about each.

The search criteria you typed are highlighted in the search results. Each search result may also provide a URL to help you navigate to the corresponding object on the inventory landing page.



NOTE: The search results are filtered on the basis of your Role-Based Access Control (RBAC) permissions. For example, if you are not assigned the "View Physical Interface" permission, then no physical interfaces are displayed on the search results page.

2. Click the URL provided with the search result to navigate to the inventory landing page of the desired object.

To filter the search results, select the relevant category or subcategories displayed on the left of the search results page.

To view the previous search results, click "Last Search Results." However, if this is your first search after logging in to Junos Space, then this link is not displayed.

To clear the search criteria in the Search field, click the close icon "x" on this field.

To dismiss the search results page, click one of the following:

- Close icon 'x' on the search results page
- **Hide Search Results** link
- Left navigation tree, search box, or any of the utility icons

If you do not enter anything in the Search field and perform a search operation, Junos Space displays the following error message:

No matching results found. Please enter another text to search.

The global search operation supports query expressions. You can search for phrases and multiple terms. The default operator for multiple terms is the OR operator.

[Table 9 on page 25](#) provides examples of query expressions that you can enter in the **Search** field.

**NOTE:**

When you enter a query expression, be aware of the following:

- You must add a back slash “\” if you want to use the following special characters in the search text:

+ ~ & || ! () { } [] ^ “ ~ * ? : \

- Field names are case-sensitive.

For example, if you have a few systems running on Junos OS 12.3 Release 4.5, then `os: 12.3R4.5` returns search results, whereas `OS: 12.3R4.5` does not return search results. This is because the field name that is indexed is “os” and not “OS.”

- If you want to search for a term that includes a space, enclose the term within double quotation marks.

For example, to search for all devices that are synchronized (that is, In Sync), enter “In Sync” in the Search field.

- You must append “*” if you want to search using partial keywords. Otherwise, the search returns 0 (zero) matches or hits.

Table 9: Supported Query Expressions in the Search Field

Query Expression	Matches Object That Contain
snmp	snmp
snmp ntp	snmp or ntp
snmp OR ntp	snmp or ntp
snmp AND ntp	snmp and ntp
protocol:snmp	snmp in the protocol field
protocol:snmp AND NOT subject:snmp	snmp in the protocol field but not in the subject field
(snmp OR ntp) AND http	http and the terms—snmp or ntp
description:“http server”	Exact phrase “http server” in the description field
description: “http server”~5	http and server within five positions of one another in the description field
ge-*	Terms that begin with “ge-,” such as ge-0/0/1 or ge-0/0/1.4
s??p	Terms such as smtp or snmp
lastmodified:[1/1/2012 TO 12/31/2012]	Last modified field values between the dates January 1, 2012 and December 31, 2012

Table 9: Supported Query Expressions in the Search Field (*continued*)

Query Expression	Matches Object That Contain
port:(80 8080 8888)	80, 8080, or 8888 in the port field
IPAddress:10.1.1.1	10.1.1.1 or 10.1.1.0/24 in the IPAddress field

Related Documentation

- [Junos Space User Interface Overview on page 9](#)

Navigating the Junos Space User Interface

This topic takes you on a quick tour of one part of the Junos Space user interface to show you how it works. Navigation is the same throughout the Junos Space Network Management Platform. Other applications within Junos Space may show some differences.

In this example, we take a path that you might follow frequently: looking at the list of all devices under management. The role and permissions that you have will govern what commands or actions are available to you.

The entire user interface is described in “[Junos Space User Interface Overview](#)” on page 9.

- [Navigating the Task Tree: The Devices Workspace on page 26](#)

Navigating the Task Tree: The Devices Workspace

Use the task tree on the left side of the display to navigate application workspaces and tasks. When you select an application, all of the task groups (also called workspaces) are displayed in the task tree.

To navigate this example:

1. In the application menu, select **Network Management Platform** if it is not already selected. (It is the default selection when you log in.)

The Platform dashboard appears in the right window. In addition, all of the task groups within Platform are shown collapsed in the task tree.

2. Select **Devices** by clicking on that name.

Graphical summaries about the devices in the network appear.

3. Expand the Devices task group by clicking the expansion symbol to the left of its name.

Tasks related to managing devices are displayed in the expanded portion of the tree. Some (for example, Discover Devices) can be further expanded.

4. Select **Manage Devices**.

A table containing data about all Junos Space devices appears. This kind of table is called an *inventory page*. If you are the first user, it might contain no data at this point. From this window, you can take various actions related to devices. You can see these

by selecting the Actions menu at the right end of the upper task bar. (All actions are shown, but only those available to you for a selected device are enabled.)

5. If there are device entries in the table, select one by clicking anywhere in its line. Mouse over the Quick View icon in the task bar to display Quick View (summary) information about the selected device.



NOTE: Icons for other tasks such as creating, modifying, and deleting items appear adjacent to the Quick View icon in some other inventory pages. The Users inventory page displays all these icons.

6. To return at any time to the next higher level of the path you have taken, select the level you want in the breadcrumbs at the top left of the window. (Pressing the Back button of your browser takes you back to your starting point, which you may or may not want.)

Notice that you can jump to any other point in the Platform application by expanding a portion of the task tree and selecting the item you want.

Related Documentation

- [Junos Space User Interface Overview on page 9](#)

Filtering Inventory Pages

On many inventory pages, you can use the Filter submenu to temporarily hide all of the entries in the table that do not match criteria that you are interested in. This feature lets you quickly find and evaluate the table entries of interest.

Many of the columns in Junos Space inventory page tables permit filtering. Depending on the table, different columns can be filtered on. [Table 10 on page 28](#) lists the tables that permit filtering.

Table 10: Filter-enabled Tables and Columns

Work-space	Page / Table		Columns
Devices	Manage Devices		All columns except: <ul style="list-style-type: none"> Physical Interfaces Logical Interfaces Connection Type
	Manage Devices	View Change Requests	All columns except: <ul style="list-style-type: none"> Creation Time Last Update Time Deployment Status
		View Space Changes	All columns except Creation Time
		View Physical Interfaces	All columns except: <ul style="list-style-type: none"> IP Address Logical Interfaces
		View Logical Interfaces	All columns except Encapsulation
		View License Inventory	All columns
		View Software Inventory	
	Add Deployed Devices		
	Add Deployed Devices	View Device Status	All columns except: <ul style="list-style-type: none"> IP Address Connection Status Managed Status
		Manage Device Adapter	All columns
Device Templates	Manage Definitions		All columns except: <ul style="list-style-type: none"> Device Family Last Update Time State
	Manage Templates		All columns except: <ul style="list-style-type: none"> Last Update Time State

Table 10: Filter-enabled Tables and Columns (*continued*)

Work-space	Page / Table	Columns
Device Images and Scripts	Manage Images	All columns except: <ul style="list-style-type: none"> • Series
	Manage Scripts	All columns except: <ul style="list-style-type: none"> • Creation Date • Last Updated Time
	Manage Operations	All columns except Priority
	Manage Operations View Operation Results	All columns
	Manage Script Bundles	All columns except: <ul style="list-style-type: none"> • Creation Date • Last Updated Time
Config Files	Manage Config Files	<ul style="list-style-type: none"> • Creation Date • Last Updated Time

To filter tables on various criteria, click the down arrow on a column header and use the Filter submenu. The choices available depend on the nature of the selected column. You can create filters that use criteria from more than one column.

Whenever you filter a table, Junos Space displays the filter criteria, including the columns being filtered, above the table. Junos Space also identifies the columns being filtered by changing their column headers to italic text.

Junos Space displays a red X to the right of the filter criteria above the table. You can clear the filter and restore the table to its original view by clicking the red X.

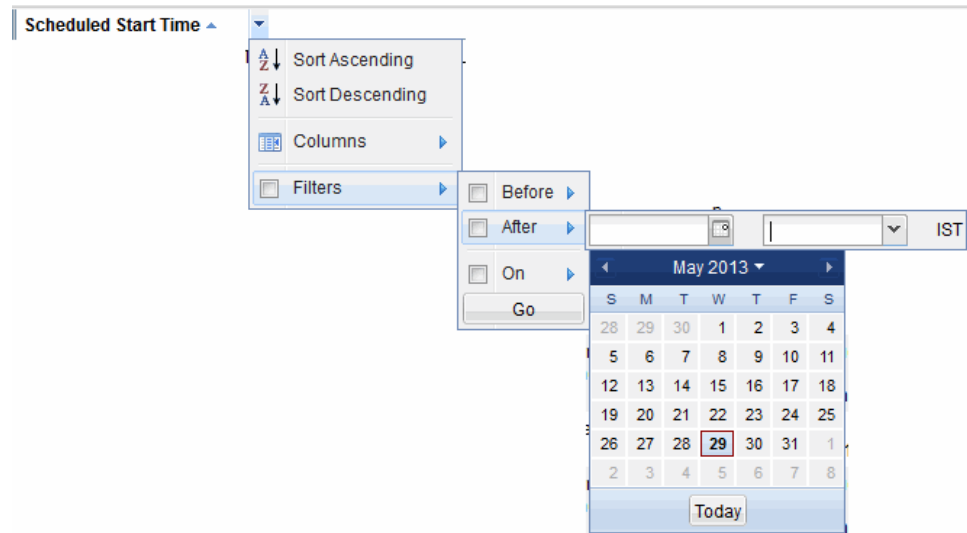
The following procedures describe how to use the different types of available filters and the different filtering features.

To filter a table on entries in a date column:

1. Click the down arrow on the column header and select **Filters**.

The Filters submenu shows a list of operators. If the column includes both dates and times, you can also use a wizard to enter the time. [Figure 10 on page 30](#) shows a typical Filter submenu for a date column.

Figure 10: Typical Submenu for a Date Column



- From the Filter submenu, select **Before**, **After**, or **On** and click the calendar icon to select the date from the calendar.

You can select both Before and After dates and times to filter the column by a specific time period. You can also select On to view events recorded on a specific date. After the selection, click **Go** to view the events on the chosen date and time. Click **Today** and specify the time to view the events that occurred today at the specified time.

To filter a table on entries in a text string column:

- Click the down arrow on the column header and select **Filters**.

The Filters submenu opens a text box.

- In the text box, type the alphanumerical string you want to filter on.

To filter a table on entries in a column of discrete elements (for example, a Status column where the only entries are “Success” and “Failure”):

- Click the down arrow on the column header and select **Filters**.

The Filters submenu opens a list of valid elements for the column.

- On the list of elements, select the check boxes for one or more elements to filter the table for only those entries.

To filter a table on entries in a column of Boolean (“true” or “false”) values:

- Click the down arrow on the column header and select **Filters**.
- Select either **True** or **False** from the Filters submenu.

To filter a table on entries in a list of numerical values:

- Click the down arrow on the column header and select **Filters**.

2. Enter values for the different operators.

You can filter a table for entries that match filters for values in multiple columns. For example, you can filter for all events on a certain date whose status was "success." When you use multiple filters, the filters are joined with logical "and."

To use multiple filters:

1. Use the Filters submenu as described previously to filter for criteria in one column.
2. Use the Filters submenu as described previously to filter for criteria in a different column.

To clear all filters and restore the table to its original unfiltered view, click the red X above the table.

To clear only the part of a filter that applies to a single column, click the down arrow on the column header and clear the check box next to Filter.

**Related
Documentation**

- [Junos Space User Interface Overview on page 9](#)

PART 2

Devices

- [Device Management Overview on page 35](#)
- [Device Configuration on page 51](#)
- [Device Inventory on page 73](#)
- [Device Operations on page 93](#)
- [Device Access on page 105](#)
- [Device Monitoring on page 119](#)
- [Custom Attributes on page 125](#)
- [Discover Devices on page 131](#)
- [Deployed Devices on page 139](#)
- [Unmanaged Devices on page 153](#)
- [Secure Console on page 157](#)
- [Manage Device Adapter on page 165](#)
- [Upload Keys to Devices on page 169](#)

CHAPTER 3

Device Management Overview

- [Device Management Overview on page 35](#)
- [Viewing Device Statistics on page 36](#)
- [Device Inventory Management Overview on page 40](#)
- [Viewing Managed Devices on page 41](#)
- [Viewing Devices and Logical Systems with QuickView on page 46](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Troubleshooting Devices on page 49](#)

Device Management Overview

You can use Junos Space Network Management Platform to simplify management of the network devices running Junos OS software.

In addition, Junos Space Network Management Platform can record the presence of non-Juniper devices, i.e. unmanaged devices in the network, thereby providing better visibility into the network, simplifying debugging and problem isolation. Junos Space Network Management Platform displays the IP address and host name of unmanaged devices. SNMP credentials and device status of unmanaged devices are not displayed; these devices' status in several categories is shown as NA. For instructions on adding unmanaged devices to Junos Space Network Management Platform, see [“Adding Unmanaged Devices” on page 153](#)

From the Devices workspace, you use device discovery to discover devices and (if the network is the system of record) synchronize device configurations with the Junos Space Network Management Platform database. You can use device discovery to discover one or many devices at a time. After Junos Space Network Management Platform discovers your network devices, you can perform the following tasks to monitor and configure devices from Junos Space Network Management Platform:

- View statistics about the managed devices in your network, including the number of devices by platform and the number of Junos family devices by release.
- View connection status and configuration status for managed devices.
- View operational and administrator status of the physical interfaces on which devices are running.

- View hardware inventory for a selected device, such as information about power supplies, chassis cards, fans, FPCs, and available PIC slots.
- If the network is the system of record, resynchronize a managed device to update the device configuration in the Junos Space Network Management Platform database to reflect that of the physical device. (If Junos Space Network Management Platform is the system of record, this capability is not available.)
- Deploy service orders to activate a service on your network devices.
- Troubleshoot devices.

Related Documentation

- [Device Discovery Overview on page 131](#)
- [Device Inventory Overview on page 40](#)
- [Discovering Devices on page 132](#)
- [Systems of Record in Junos Space Overview on page 733](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Viewing Managed Devices on page 41](#)
- [Exporting License Inventory on page 80](#)
- [Troubleshooting Devices on page 49](#)

Viewing Device Statistics

The Devices statistics page provides three types of data for managed devices:

- Device Count by Platform—The number of Juniper Networks devices organized by type
- Device Status—The connection status of managed devices on the network
- Device Count by OS—The number of devices running a particular Junos OS release

To view device statistics, select **Platform > Devices**.

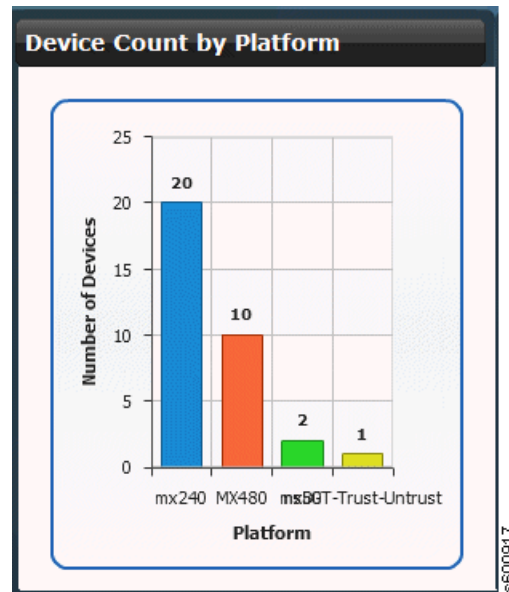
This topic includes the following tasks:

- [Viewing the Number of Devices by Platform on page 37](#)
- [Viewing Connection Status for Devices on page 37](#)
- [Viewing Devices by Junos OS Release on page 38](#)

Viewing the Number of Devices by Platform

Figure 11 on page 37 shows the Device Count by Platform report. The bar chart shows the number of Juniper Networks devices on the y axis discovered by platform type on the x axis. Each vertical bar in the chart displays the number of managed devices for a platform.

Figure 11: Device Count by Platform Report



To view more detailed information about devices per platform:

- Click a bar in the bar graph. The Device Management inventory page appears filtered by the device type you selected. See [“Viewing Managed Devices” on page 41](#).

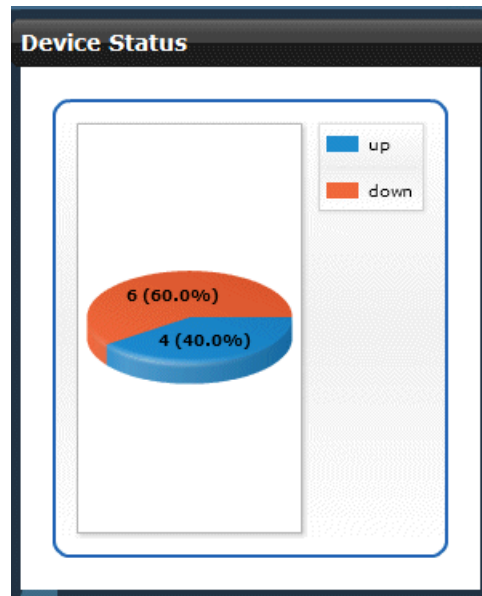
To save the bar chart as an image or to print for presentations or reporting:

- Right-click the bar chart and use the menu to save or print the image.

Viewing Connection Status for Devices

Figure 12 on page 38 shows the Device Status report. The pie chart displays the percentage and number of devices that are connected and disconnected on the network. The up or down status is expressed as a percentage of the total number of devices.

Figure 12: Device Status Report



To view more detailed device status information:

- Click a slice in the pie chart. The Device Management inventory page appears filtered by the devices that are up or down. See "[Viewing Managed Devices](#)" on page 41.

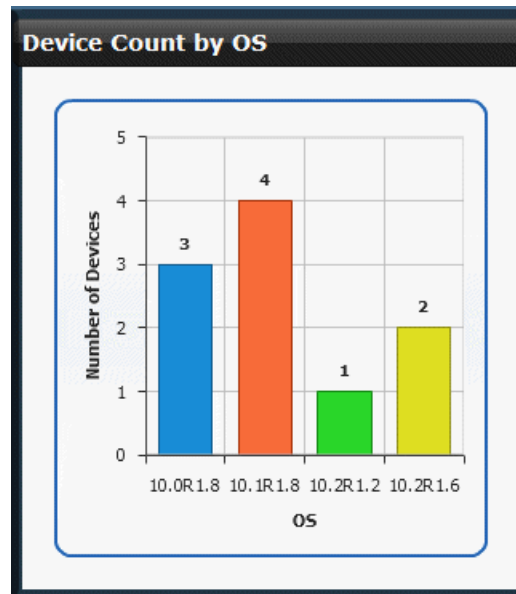
To save the pie chart as an image or to print for presentations or reporting:

- Right-click the bar chart and use the menu to save or print the image.

Viewing Devices by Junos OS Release

Figure 13 on page 39 shows the Device Count by OS report. The bar chart shows the number of Juniper Networks devices on the network (the y axis) categorized by running a certain Junos OS release (the x axis).

Figure 13: Device Count by OS Report



To view more detailed information about devices running a particular Junos OS release:

- Click a bar in the chart. The Device Management inventory page appears. See [“Viewing Managed Devices” on page 41](#).

To save the pie chart as an image or to print for presentations or reporting:

- Right-click the bar chart and use the menu to save or print the image.

Related Documentation

- [Viewing Managed Devices on page 41](#)
- [Viewing Physical Inventory on page 73](#)
- [Discovering Devices on page 132](#)

Device Inventory Management Overview

You manage device inventory through the Device Management application in the Devices workspace. From the Device Management inventory you can perform several functions:

- List the device inventory to view information about the hardware and software components of each device that Junos Space manages.
- View information about the scripts associated with the devices and details of script execution on devices.
- View information about the service contract or end-of-life status for a part.
- View the operational and administrator status for the physical interfaces on which devices are run.
- Change credentials for a device.
- View location and ship-to-address of a device if address groups are configured in Service Now.
- Export the device inventory information for use in other applications, such as those used for asset management.
- Troubleshoot a device.
- If the network is the system of record, resynchronize the network devices managed by Junos Space Network Management Platform.

The device inventory in the Junos Space Network Management Platform database is generated when the device is first discovered and synchronized in Junos Space Network Management Platform. After a device is synchronized, the device inventory in the Junos Space Network Management Platform database matches the inventory on the device itself.

If either the physical (hardware) or logical (config) inventory on the device is changed, then the inventory on the device is no longer synchronized with the Junos Space Network Management Platform database. However, Junos Space Network Management Platform automatically triggers a resync job when a configuration change request commit or out-of-band CLI commit occurs on a managed device.

You can also manually resynchronize the Junos Space Network Management Platform database with the physical device by using the **Resynchronize with Network** command from the Devices workspace in the Junos Space Network Management Platform user interface.

If Junos Space Network Management Platform is the system of record, the database values have precedence over any out-of-band changes to network device configuration, and neither manual nor automatic resynchronization is available.

To reach the device management applications, select **Devices > Device Management**.

Related Documentation

- [Device Management Overview on page 35](#)
- [Device Discovery Overview on page 131](#)

- [Viewing Physical Inventory on page 73](#)
- [Systems of Record in Junos Space Overview on page 733](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Exporting Physical Inventory Information on page 86](#)
- [Exporting License Inventory on page 80](#)
- [Troubleshooting Devices on page 49](#)

Viewing Managed Devices

You can view operating system, platform, IP-address, license, connection status, and several other types of information for all the managed devices in your network. Device information is displayed in a table. Unmanaged devices are also shown, but without status and some other information.

You can also view managed devices from the Network Monitoring workspace, via the Node List (see [“Viewing the Node List” on page 371](#)). If the network is the system of reference, the Network Monitoring workspace also enables you to resync your managed devices (see [“Resyncing Nodes” on page 372](#)).

Neither manual nor automatic resynchronization occurs when Junos Space Network Management Platform is the system of reference. See [“Systems of Record in Junos Space Overview” on page 733](#).

- [Viewing Devices on page 42](#)

Viewing Devices

To view configuration and run-time information for devices:

1. Select **Devices > Device Management**.
The Device Management page appears.

Figure 14: Device Management Page

Name	Physical Inter...	Logical Interf...	OS Version	Device Family	Platform	IP Address	Connection S...	Managed Stat...	AIS Install Pa...	Event Profile
1 10.205.56.3	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.3	up	In Sync	---	---
1 10.205.56.4	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.4	up	In Sync	---	---
10.205.56.3 & LSYs(a)	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.3	up	In Sync	---	---
10.205.56.4 & LSYs(a)	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.4	up	In Sync	---	---
3 10.205.56.3	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.3	up	In Sync	---	---
3 10.205.56.4	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.4	up	In Sync	---	---
4 10.205.56.3	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.3	up	In Sync	---	---
4 10.205.56.4	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.4	up	In Sync	---	---
Austin	View	View	12.3-2012110...	junos	MX80	10.155.69.43	up	Out Of Sync	---	---
Bangalore	View	View	11.2R3.3	junos	M71	10.205.56.9	up	Out Of Sync	---	---
CE-EX-London	View	View	12.2R3.5	junos-ex	EX4200-48T	10.155.69.105	up	Out Of Sync	---	---
Lays-One 10.205.56.3	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.3	up	In Sync	---	---
Lays-One 10.205.56.4	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.4	up	In Sync	---	---
Mx-80	View	View	12.1R3.5	junos	MX80	10.155.69.42	up	Out Of Sync	---	---
Mumbai	View	View	11.2R3.3	junos	M320	10.205.56.5	up	Out Of Sync	---	---
SFO-RE0	View	View	12.3R2.1	junos	MX960	10.155.69.13	up	Out Of Sync	---	---
SFO-RE0	View	View	12.3R2.1	junos	MX960	10.155.69.221	up	Out Of Sync	---	---
aldergrove-sn220	View	View	12.3R2.5	junos-es	SRX220H-POE	10.155.69.63	up	Out Of Sync	---	---
atherton-VC1	View	View	12.3R1.7	junos-ex	EX3300-24T	10.155.69.134	up	Out Of Sync	---	---
atherton-VC1	View	View	12.3R1.7	junos-ex	EX3300-24T	10.155.69.133	up	Out Of Sync	---	---
boston-ex4500	View	View	11.3R7	junos-ex	EX4500-40F	10.155.69.77	up	Out Of Sync	---	---
delaware-ex4500	View	View	12.2R2.4	junos-ex	EX4500-40F	10.155.69.116	up	Out Of Sync	---	---
delaware-re0	View	View	12.3R3.1	junos	MX480	10.155.69.117	up	Out Of Sync	---	---
delaware-re0	View	View	12.3R3.1	junos	MX480	10.155.69.17	up	Out Of Sync	---	---
dev-sn3400 & LSYs(a)	View	View	11.4R1.6	junos-es	SRX3400	10.155.69.246	up	Out Of Sync	---	---
ex-4200-pork	View	View	12.2R3.5	junos-ex	EX4200-24T	10.155.69.32	up	Out Of Sync	---	---

Table 11 on page 43 describes the fields displayed in the inventory window. In the table, an asterisk indicates that this column is not shown by default.

Table 11: Fields in the Device Management Table

Field	Description
Name	The device configuration name.
Physical Interfaces	Link to the view of physical interfaces for the device. (NA for an unmanaged device.)
Logical Interfaces	Link to the view of logical interfaces for the device. (NA for an unmanaged device.)
OS Version	Operating system firmware version running on the device. (Unknown for an unmanaged device.)
Device Family	Device family of the selected device. (For an unmanaged device, this is the same as the vendor name you have provided. It is shown as Unknown if no vendor name was provided and if SNMP is not used or has failed.)
Platform	Model number of the device. (For an unmanaged device, the platform is discovered through SNMP. If it cannot be discovered it is shown as Unknown.)
Vendor*	The device vendor. (For an unmanaged device, the vendor name is displayed as Unknown if the vendor name was not provided and it cannot be discovered through SNMP.)
Schema Version*	The DMI schema version that Junos Space Network Management Platform has for this device. (Unknown for an unmanaged device.) See “Managing DMI Schemas Overview” on page 714 .
IP Address	IP address of the device.
Connection Status	<p>Connection status of the device in Junos Space. Values differ between network as system of record (NSOR) and Junos Space as system of record (SSOR).</p> <ul style="list-style-type: none"> up—Device is connected to Junos Space Network Management Platform. When connection status is up, in NSOR, the managed status is Out of Sync, Synchronizing, In Sync, or Sync Failed. In SSOR, status is In Sync, Device Changed, Space Changed, Both Changed, or Unknown (which usually means connecting). down—Device is not connected to Junos Space Network Management Platform. When Connection status is down, the managed status is None or Connecting. NA—The device is unmanaged.

Table 11: Fields in the Device Management Table (*continued*)

Field	Description
Managed Status	<p>Current status of the managed device in Junos Space Network Management Platform:</p> <ul style="list-style-type: none"> Connecting—Junos Space Network Management Platform has sent connection RPC and is waiting for first connection from device. In Sync—Sync operation has completed successfully, and Junos Space Network Management Platform and the device are synchronized. None—Device is discovered, but Junos Space Network Management Platform has not yet sent connection RPC. Out of Sync—In NSOR, device has connected to Junos Space Network Management Platform, but the sync operation has not been initiated, or an out-of-band configuration change on the device was detected and auto-resync is disabled or has not yet started. Device Changed, Space Changed, Both Changed—In SSOR, Junos Space Network Management Platform and the device are not in sync, and the party that has been changed is noted. Neither automatic nor manual resync is available. Synchronizing—Sync operation has started because of device discovery, a manual re-sync operation, or an automatic re-sync operation. Sync Failed—Sync operation failed. Unmanaged—Device is unmanaged.
Authentication Status	<ul style="list-style-type: none"> Key Based—Authentication key was successfully uploaded. Credential—Key upload was not attempted; login to this device is by credentials. Key Conflict—Device was not available; key upload was unsuccessful. NA—Device is unmanaged.
Serial Number*	Serial number of the device chassis. (Unknown for an unmanaged device.)
Connection Type*	Current connection status for the device: Up, Out of Sync, Down, or Unknown. (See Table 12 on page 44).
AIS Install Package Version*	Version of the script used to install a bundle of applications via the event profile feature of the Service Now application.. ('—' if not used.)
Event Profile*	Name of the event profile installed via the Service Now application. ('—' is none is installed.)

[Table 12 on page 44](#) describes the connection status icons.

Table 12: Device Connection Status Icon





Icon	Description
	<p>Connection is up—The device is connected to Junos Space Network Management Platform and is running properly.</p> <p>NOTE: Before you can update a device from Junos Space Network Management Platform (deploy service orders), the device connection must be up.</p>
	<p>Out of sync—The device is connected to Junos Space Network Management Platform but the device configuration in the Junos Space Network Management Platform database is out of sync with the physical device.</p>

Table 12: Device Connection Status Icon (*continued*)

Icon	Description
	Connection is down—The device is not currently connected to Junos Space Network Management Platform or an event has occurred, either manually by an administrator or automatically by the flow of a type of traffic, that has stopped the device from running.
	The device is unmanaged. Status is not available.

2. Sort the table by mousing over the column header for the data you want to sort by and clicking the down arrow. Select **Sort Ascending** or **Sort Descending**.
3. Show columns not in the default table view, or hide columns, as follows:
 1. Mouse over any column header and click the down arrow.
 2. Select **Columns** from the menu.
 3. Select the check boxes for columns that you want to view. Clear the check boxes for columns that you want to hide.
4. View information about devices as follows:
 - To restrict the display of devices, enter a search criterion of one or more characters in the Search bar and press Enter.
All devices that match the search criterion are shown in the main display area.
 - To view hardware inventory information for a device, select the row for the device, and select **Device Inventory > View Physical Inventory** from the Actions menu or the right-click menu.
 - To view the physical or logical interfaces for a device, select the View link in the appropriate column and row for the device.

For information about filtering rows to see information about only those devices of interest, see [“Filtering Inventory Pages” on page 27](#). You can filter for unmanaged devices only in those columns that contain resolved values.

Related Documentation

- [Viewing Device Statistics on page 36](#)
- [Viewing Physical Inventory on page 73](#)
- [Exporting License Inventory on page 80](#)
- [Viewing Physical Interfaces on page 76](#)
- [Discovering Devices on page 132](#)
- [Viewing the Node List on page 371](#)
- [Filtering Inventory Pages on page 27](#)
- [Junos Space User Interface Overview on page 9](#)
- [Resyncing Nodes on page 372](#)

- [Systems of Record in Junos Space Overview on page 733](#)

Viewing Devices and Logical Systems with QuickView

The QuickView feature shows you the type and status of a device or logical system using an icon.

To view a device or logical system using Quick View:

1. Select **Network Application Platform > Devices > Device Management**.
2. Select the Quick View action button on the menu bar.
3. Alternatively, at the right edge of the Platform window, find the sidebar open arrow for the Device Management table.



NOTE: Be careful to find the correct sidebar open arrow. There are two; one on the left that opens the Quick View sidebar, and one on the right that opens the Help panel.

The Quick View sidebar arrow in green. The other arrow, highlighted in red, opens the Help sidebar.

4. Click the Quick View sidebar open arrow.

Platform opens the Quick View sidebar. The Quick View shows the status of the device that is currently selected in the table.

You can close the Quick View window in the same way that you opened it.

Related Documentation

- [Understanding Logical Systems for SRX Series Services Gateways on page 97](#)
- [Viewing the Physical Device for a Logical System on page 99](#)
- [Viewing Logical Systems for a Physical Device on page 100](#)
- [Junos Space User Interface Overview on page 9](#)
- [Creating a Logical System \(LSYS\) on page 98](#)
- [Deleting Logical Systems on page 99](#)
- [*Junos OS Logical Systems Configuration Guide for Security Devices*](#)

Understanding How Junos Space Automatically Resynchronizes Managed Devices

When configuration changes are made on a physical device that Junos Space Network Management Platform manages, Junos Space Network Management Platform reacts differently depending on whether the network itself is the system of record (NSOR) or Junos Space Network Management Platform is the system of record (SSOR).

In the NSOR case, Junos Space Network Management Platform receives a system log message and automatically resynchronizes with the device. This ensures that the device inventory information in the Junos Space Network Management Platform database matches the current configuration information on the device.

In the SSOR case, the Junos Space Network Management Platform receives a system log message from device after the device change is committed. Managed status for that device changes to out-of-sync, but no resynchronization occurs. The Junos Space Network Management Platform administrator has the option of resetting the network device's configuration to the Junos Space Network Management Platform database values or not doing so.

This topic covers:

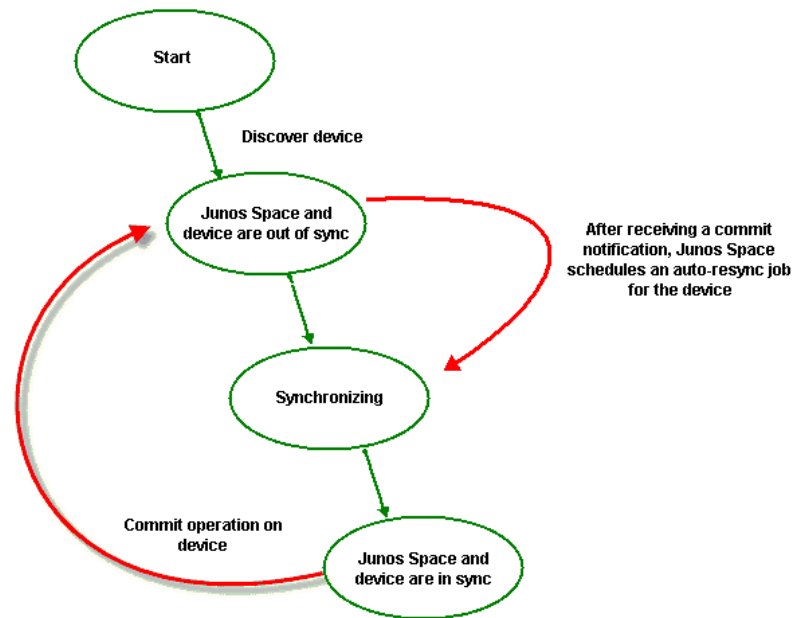
- [Network as System of Record on page 47](#)
- [Junos Space as System of Record on page 49](#)

Network as System of Record

After Junos Space Network Management Platform discovers and imports a device, if the network is the system of record, Junos Space Network Management Platform enables the auto-resync feature on the physical device by initiating a commit operation.

After auto-resynchronization is enabled, any configuration changes made on the physical device, including out-of-band CLI commits and change-request updates, automatically trigger resynchronization on the device. [Figure 15 on page 48](#) shows how a commit operation on the device triggers resynchronization.

Figure 15: Resynchronization Process



When a commit operation is performed on a managed device under NSOR, Junos Space Network Management Platform, by default, schedules a resync job to run 20 seconds after the commit operation is received. However, if Junos Space Network Management Platform receives another commit notification within 20 seconds of the previous commit notification, no additional resync jobs are scheduled because Junos Space Network Management Platform resynchronizes both commit operations in one job. This damping feature of automatic resynchronization provides a window of time during which multiple commit operations can be executed on the device, but only one or a few resync jobs are required to resynchronize the Junos Space Network Management Platform database after multiple configuration changes are executed on the device.

You can change the default value of 20 seconds to any other duration by specifying the value in seconds in the **Administration > Applications > Network Management Platform > Modify Application Settings > Device > Max auto resync waiting time secs** field. For example, if you set the value of this field to 120 seconds, then Junos Space Network Management Platform automatically schedules a resync job to run 120 seconds after the first commit operation is received. If Junos Space Network Management Platform receives any other commit notification within these 120 seconds, it resynchronizes both commit operations in one job.

When Junos Space Network Management Platform receives the device commit notification, the device status is “Out of Sync”. When the resync job begins on the device, the Managed Status for the device displays “Synchronizing” and then “In Sync” after the resync job has completed, unless a pending device commit operation causes the device to display “Out of Sync” while it was synchronizing.

When a resync job is scheduled to run but another resync job on the same device is in progress, Junos Space Network Management Platform delays the scheduled resync job. The time delay is determined by the damper interval that you can set from the application workspace. By default, the time delay is 20 seconds. The scheduled job is delayed as long as the other resync job to the same device is in progress. When the currently running job finishes, the scheduled resync job starts.

You can disable the auto-resync feature in the Application workspace. When auto-resync is turned off, the server continues to receive notifications and will go into the out-of-sync state; however, the auto-resync does not run on the device. To resynchronize a device when the auto-resync feature is disabled, you can use the resync feature to manually resync the device.

For information about setting the damper interval to change the resync time delay and information about disabling the auto-resync feature, see [“Modifying Junos Space Application Settings” on page 624](#).

Junos Space as System of Record

If Junos Space Network Management Platform is the system of record, the automatic resynchronization described above does not occur. When Junos Space Network Management Platform receive the device commit notification, device status becomes Out of Sync and remains so unless you push the system-of-record configuration from the Junos Space Network Management Platform database down to the device.

Related Documentation

- [Systems of Record in Junos Space Overview on page 733](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Device Discovery Overview on page 131](#)
- [Device Inventory Overview on page 40](#)
- [Viewing Managed Devices on page 41](#)

Troubleshooting Devices

You can check the configuration settings of one or more devices from Junos Space Network Management Platform using Looking Glass. It enables you to execute **show** commands across multiple devices to compare the configuration and runtime information. See [“Using Looking Glass” on page 96](#).

In Junos Space Network Management Platform you can also perform troubleshooting on N-PE devices from Network Activate. See the Troubleshooting N-PE Devices Before Provisioning a Service topic in the Network Activate documentation.

Related Documentation

- [Deploying Device Instances on page 149](#)

CHAPTER 4

Device Configuration

- [Viewing Active Configuration on page 52](#)
- [Adding Configuration Filters on page 53](#)
- [Modifying Device Configuration Overview on page 53](#)
- [Selecting the Device and the Configuration Perspective on page 54](#)
- [Modifying the Configuration on the Device on page 55](#)
- [Modifying Unmanaged Device Configuration on page 57](#)
- [Reviewing and Deploying the Device Configuration on page 57](#)
- [Configuration Guides Overview on page 63](#)
- [Saving the Configuration Created using the Configuration Guides on page 63](#)
- [Deploying the Configuration Created using the Configuration Guides on page 64](#)
- [Previewing the Configuration Created using the Configuration Guides on page 64](#)
- [Resolving Out-of-Band Configuration Changes on page 65](#)
- [Viewing Configuration Change Log on page 66](#)
- [Viewing Assigned Shared Objects on page 68](#)
- [Viewing Template Deployment \(Devices\) on page 70](#)

Viewing Active Configuration

This action enables you to view the current configuration on the device. To display all of a device's configuration options, Junos Space Network Management Platform requires the DMI schema for that device type. To upload a DMI schema to Junos Space Network Management Platform, see [Managing DMI Schemas Overview](#).

If Junos Space Network Management Platform does not have the DMI schema for that device type, it uses a default DMI schema. The default DMI schema does not necessarily display all your device's configuration options, whereas having the DMI schema specific to that device enables Junos Space Network Management Platform to let you view all of the device's configuration options. If Junos Space Network Management Platform uses the default schema, some already configured parameters on the device might not be displayed. To view the active configuration:

1. Select **Network Application Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device whose configuration you want to view and select **View Active Configuration** from the contextual menu.

The **View Active Configuration** page is displayed.

In this page, The left pane shows the Junos OS statement hierarchy and the right pane shows the active configuration in the XML view.

3. Use the expander buttons (plus and minus) to explore the Junos OS statement hierarchy.
4. See which configuration options in the hierarchy are actually set by selecting **Configured Data** from the Perspective list on the top of the left pane next to the magnifying glass search icon.
5. Select the Settings icon to modify the custom settings related to Multi-select and Autorefresh.
6. Select the Create Filter icon to add a configuration filter.
7. Search for a particular option. See [Finding Configuration Options](#). Although that topic deals with Device Templates, the principle is exactly the same.

Related Documentation

- [Modifying Device Configuration Overview on page 53](#)

Adding Configuration Filters

This option allows creating new filter using the DMI schema for the device types. Filter name is a unique identifier for the filter and device family is used to define a filter based on the DMI schema for the device type. Create Filter GUI has two trees, one is the DMI schema tree which has Junos OS statement hierarchy for the device family selected above. Right side tree is the filtered tree constructed by selecting the nodes in the Junos OS statement hierarchy.

To add a configuration filter:

1. Select a node from the left side tree to make it available at right side tree. Selecting of any node intern selects all its children and expands the node using expander buttons (plus).
2. Selected children will be displayed at both the trees only if you expand that node.
3. Change the device family in the selection list to reload the left side tree with that particular DMI schema for the device type.
4. Select a filter from the Filter Selection-list to filter Configuration Tree.

Related Documentation

- [Viewing Active Configuration on page 52](#)

Modifying Device Configuration Overview

This action enables you to view and modify a device's configuration. To display all configuration options of a device, Junos Space Network Management Platform requires the DMI schema for that device type. To upload a DMI schema to Junos Space Network Management Platform, see [“Managing DMI Schemas Overview” on page 714](#).

If Junos Space Network Management Platform does not have the DMI schema for that device type, it uses a default DMI schema. The default DMI schema does not necessarily display all configuration options of the device, whereas having the DMI schema specific to that device enables Junos Space Network Management Platform to let you edit all configuration options of the device. If Junos Space Network Management Platform uses the default schema, some already configured parameters on the device might not be displayed.

Junos Space Network Management Platform checks for an exact match between the device and DMI schema every time you edit the configuration of the device.

You can edit the configuration on the device using the schema-based Configuration Editor or Configuration Guides. To know more about Configuration Guides, see [“Configuration Guides Overview” on page 63](#).

The sequence of tasks to edit a device configuration is as follows:

1. [Selecting the Device and the Configuration Perspective on page 54](#)
2. [Modifying the Configuration on the Device on page 55](#)

The Junos OS devices can maintain up to 49 copies of a configuration file. Junos Space Network Management Platform provides database management of configuration files (see [“Systems of Record in Junos Space Overview” on page 733](#)).

- Related Documentation**
- [Managing Configuration Files Overview on page 444](#)
 - [Managing DMI Schemas Overview on page 714](#)

Selecting the Device and the Configuration Perspective

You can modify the device configuration using the Schema-based Configuration Editor. The Modify Configuration page shows the DMI schema applied by Junos Space Network Management Platform to the selected device. If Junos Space Network Management Platform has the same DMI schema as the device, then that schema will be applied. If Junos Space Network Management Platform does not then it displays the default schema for the selected device's type. The default schema does not necessarily show all of the configuration options available in the actual device schema. Therefore, you cannot configure those options by using Junos Space Network Management Platform; you must go to the device itself. To avoid this situation, upload the device's schema to Junos Space Network Management Platform using the DMI Schema management workspace (see [“Managing DMI Schemas Overview” on page 714](#)).

This topic describes how to select the device and the configuration perspective before editing the configuration.

To select the device and the perspective:

1. Select **Devices > Device Management**, and select a single device.
2. From the Actions menu, select **Device Configuration > Modify Configuration**.

The Modify Configuration page is displayed. The default perspective is All Data, which means all configuration options, whether set or not. The left pane shows the Junos OS statement hierarchy. The right pane shows the values in the running configuration.

3. Explore the configuration details in the following ways:
 - Use the expander buttons (plus and minus) to explore the Junos OS statement hierarchy.
 - Mouse over the blue information icon next to each Junos OS statement to display explanatory text. The information is the same as that in the device CLI.
 - See which configuration options in the hierarchy are actually set by selecting **Configured Data** from the Perspective list on the top of the left pane next to the magnifying glass search icon.
 - Likewise, in the right pane, select **Configured Data** on the list at the right of the title bar to display in the right pane only those options that are actually configured.
 - Search for a particular option. For more information about searching for a particular option, see [“Finding Configuration Options” on page 199](#). Although that topic deals with Device Templates, the principle is exactly the same.

- Related Documentation**
- [Modifying Device Configuration Overview on page 53](#)
 - [Modifying the Configuration on the Device on page 55](#)
 - [Updating a DMI Schema on page 716](#)

Modifying the Configuration on the Device

You can modify the configuration on a device from the View/Edit Configuration page. This topic describes the individual operations involved in modifying a device configuration after you have selected your device and the configuration perspective.

To modify a configuration option:

1. Select **Network Application Platform > Devices > Device Management**.
The Device Management page is displayed.
2. Right-click the device whose configuration you want to modify and select **View/Edit Configuration**.
The **View/Edit Configuration** page is displayed.
3. Select a configuration option from the hierarchy in the left pane.

The contents of the right pane changes to reflect your selection on the left, and the full name of the configuration option appears on the title bar on the right pane.

The parameters of a configuration option are displayed varies depending on the data type of the option. The data type is shown in a tooltip when you mouse over an option in the hierarchy. It is the data type that determines how the parameter is validated, and the data type is in turn determined by the DMI schema.

The options displayed in table rows can be manipulated as follows:

- Edited by selecting a row and selecting the diagonal pencil icon
- Added by selecting the plus icon
- Deleted by selecting a row and selecting the minus icon

The variety in the data presentation only affects how you arrive at the value you want to change, not the value itself.

For more information about the correlation between data types and validation methods, see [“Creating a Template Definition” on page 189](#).

A parameter available for configuration is usually displayed as a link called **View/Configure**.

4. Select **View/Configure** until you arrive at the parameter that you want to change.
5. Make your change.

In the hierarchy on the left, the option you have changed is highlighted, and the option label is in bold. This distinguishes it from subsequent options that you simply visit, without making any changes. If you have opened up the hierarchy, you can see not

only the name of the principal option, but also the name of the particular parameter that you have changed- for example not only “SNMP,” but also “Description.”



NOTE: Your edits are saved when you click anywhere else on the Edit Device Configuration page, whether another configuration option or any of the buttons.

6. (Optional) For information about individual parameters, click the little blue information icons to the right of the configuration settings to display the explanations.
7. (Optional) To add comments about individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.
8. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.



NOTE: You can activate or deactivate a configuration option only if the configuration node exists.

9. (Optional) Enter in the **Comments** field any remarks that you want to be seen when the consolidated configuration is reviewed. The remarks appear as a title for the configuration.

If you do not enter anything in this field, the label for the configuration is only something similar to **Generated config change from: created by super at 2012-09-14 01:33:26.564 (1 Item)**.

10. Click **OK**.

The Device Management page reappears.

Related Documentation

- [Modifying Device Configuration Overview on page 53](#)
- [Selecting the Device and the Configuration Perspective on page 54](#)
- [Managing DMI Schemas Overview on page 714](#)
- [Creating a Template Definition on page 189](#)

Modifying Unmanaged Device Configuration

In the Junos Space Network Management Platform context, unmanaged devices are those made by vendors other than Juniper Networks, Inc. You can add such devices to Junos Space Network Management Platform manually, or by importing multiple devices simultaneously from a CSV file.

To modify the configuration on a non-Juniper device:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed. This page lists the unmanaged devices added to Junos Space Network Management Platform.

2. Right-click the unmanaged device whose configuration you want to modify and select **View/Edit Unmanaged Device Configuration**. The Modify Unmanaged Device Configuration page is displayed.
3. Modify the loopback address in the **Loopback address** field.
4. Modify the loopback name in the **Loopback Name** field.
5. Click **Save**.

A job is created. Click the Job ID to view the job details.

Related Documentation

- [Device Management Overview on page 35](#)
- [Viewing Managed Devices on page 41](#)

Reviewing and Deploying the Device Configuration

When you finish modifying a device configuration, you can review and deploy the configuration using the Review/Deploy Configuration page. You can review and deploy configurations created using the Schema-based Configuration Editor or the Configuration Guides. You can review these configurations in a device-centric view, approve or reject appropriate configuration changes, and deploy them to one or more devices in a single commit operation.

In Junos Space Network Management Platform, different users can create configuration templates for a particular device. A single reviewer can then view all of these configurations for multiple devices (see [“Viewing Assigned Shared Objects” on page 68](#)) to decide which of them to deploy, and in which sequence.



NOTE: It is possible to create a configuration that is not shared, in which case, only its creator can deploy it. For example, configurations scheduled for deployment that were created with the Schema-based Configuration Editor are not shared, and are therefore not visible as a shared object.

You can perform the following tasks on the Review/Deploy Configuration page:

- [Viewing the Device Configuration Changes on page 58](#)
- [Validating the Configuration on the Device on page 59](#)
- [View the Device-Configuration Validation Report on page 59](#)
- [Excluding or Including a Group of Configuration Changes on page 60](#)
- [Deleting a Group of Configuration Changes on page 60](#)
- [Approving the Configuration Changes on page 61](#)
- [Rejecting the Configuration Changes on page 61](#)
- [Deploying the Configuration Changes on page 62](#)

Viewing the Device Configuration Changes

You can view the configuration changes you want to deploy on the device, on the Review/Deploy Configuration page. To view the configuration changes:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.

The Review/Deploy Configuration page is displayed. The Select Devices section on the left side of this page displays the device on which you are about to deploy to the configuration. The right side of this page displays the modified configuration that you are about to deploy on the device.



NOTE: You can also select multiple devices and view the configuration changes on these devices in the Change Summary tab.

The following table show the columns displayed in the Select Devices section.

Table 13: Selected Devices Columns

Column Name	Description
Device ID	ID of the device.
Device Name	Name of the device.
Validation	Validation results of the configuration on the device.
Status	Status of the modified configuration - approved, rejected, or deployed on the device.

The right side of the page displays different tabs to view the configuration deltas from the running configuration. Delta is the differential configuration that you are about to deploy on the device. The following table lists the tabs.

Table Name	Description
Change Summary	Pending configuration changes for the device.
Delta Config (CLI)	Deltas from the running configuration in CLI.
Delta Config (XML)	Deltas from the running configuration in XML.
Additional Info	Add comments to the audit trail.

3. Click the **Delta Config (CLI)** tab to view deltas from the running configuration in CLI format.
4. Click the **Delta Config (XML)** tab to view deltas from the running configuration in XML format.
5. Click the **Additional Info** tab to add comments to the audit trail in the Comments section.

Validating the Configuration on the Device

You can validate the delta configuration on the device and view the validation results before deploying the configuration changes to the device. To validate the delta configuration on the device:

1. Select **Network Application Platform > Devices > Device Management**.
The Device Management page appears.
2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.
The Review/Deploy Configuration page is displayed.
3. In the Change Summary tab, click the **Validate on Device** link.
A job is created. You can click the Job ID to view the job details.

View the Device-Configuration Validation Report

When you complete validating the configuration on the device, you can view the validation results. To view the validation results:

1. Select **Network Management Platform > Devices > Device Management**.
The Device Management page appears.
2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.
The Review/Deploy Configuration page is displayed.

3. On the Change Summary tab, click the **Device Validation Report** link.
A pop-up window displays the results of the validation.
4. Click **Close**.

Excluding or Including a Group of Configuration Changes

You can exclude or include a specific group of configuration changes. If you exclude the configuration change, the change will not be deployed to the device during the deploy operation. To exclude or include a specific group of configuration changes:

1. Select **Network Management Platform > Devices > Device Management**.
The Device Management page appears.
2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.
The Review/Deploy Configuration page is displayed.
3. On the Change Summary tab, click **Exclude** to exclude changes in the template or changes from the Schema-based Configuration Editor.
4. On the Change Summary tab, click **Include** to include any template changes to the configuration that you are deploying to the device.
5. Click **Close**.

Deleting a Group of Configuration Changes

You can delete a specific group of configuration changes. If you delete the configuration change, the change is not deployed to the device during the deploy operation. To delete a specific group of configuration changes:

1. Select **Network Management Platform > Devices > Device Management**.
The Device Management page appears.
2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.
The Review/Deploy Configuration page is displayed.
3. On the Change Summary tab, click **Delete** to delete any changes from the Schema-based Configuration Editor.
4. Click **Close**.

Approving the Configuration Changes

You can approve the configuration changes after you have successfully validated the configuration changes on the device. Approving the configuration is the last step you perform before you deploy the configuration on the device. To approve the configuration:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.

The Review/Deploy Configuration page is displayed.

3. Click **Approve** to approve the configuration.
4. Click **Yes** on the confirmation pop-up window.



NOTE: If you cannot approve the configuration on the Review/Deploy Configuration page, check if the **Enable approval workflow for configuration deployment** check box at **Administration > Applications > Modify Application Settings > Devices** is not selected. By default, this check box is selected.

Rejecting the Configuration Changes

You can reject the configuration changes you have approved earlier. Rejecting the configuration changes prevents the configuration from being deployed on the device. To reject the configuration:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.

The Review/Deploy Configuration page is displayed.

3. Select an approved configuration change and click **Reject**.
4. Click **Yes** on the confirmation pop-up window.

Deploying the Configuration Changes

You can deploy the configuration changes you have approved earlier. Deploying the configuration changes pushes the configuration from being deployed on the device. To deploy the configuration:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Review/Deploy Configuration**.

The Review/Deploy Configuration page is displayed.

3. Click **Deploy**.

The Deploy Configuration pop-up window is displayed. You can deploy the configuration immediately or schedule to deploy the configuration at a later point in time.

4. To deploy the configuration to the device immediately, select the **Deploy Now** option button.
5. To schedule a deployment, select **Deploy Later** and specify the schedule.
6. Click **OK**.



NOTE: If you are upgrading to Junos Space Network Management Platform 13.1 from an earlier version, you should deploy all consolidated configurations and change requests before the upgrade. The upgrade deletes all consolidated configurations and change requests.

Related Documentation

- [Viewing Assigned Shared Objects on page 68](#)
- [Assigning a Device Template to Devices on page 220](#)

Configuration Guides Overview

The Device Management Interface (DMI) schema-based Configuration Editor that is shipped with Junos Space Network Management Platform helps you modify the entire configuration of a device. However, to modify only a part of the configuration of the device, use the custom-built user interface of Configuration Guides.

Configuration Guides are deployed as a single application on the Junos Space Network Management Platform. When you install Junos Space Network Management Platform on a device, the Configuration Guides packaged in the application are automatically displayed on the View/Edit Configuration page. All changes to the device configuration you made using the Configuration Guides are collected as a single change request. The configuration changes you make in one Configuration Guide are visible in other Configuration Guides and the Configuration Editor. If you change a parameter using two Configuration Guides, the change made in the last Configuration Guide is accepted. The changes are merged in chronological order. You can preview the combined configuration changes in XML and CLI formats.

When you have finished editing the device configuration using the Configuration Guides, you can finalize the changes by previewing and saving the changes, or by deploying the changes on the device. Clicking the Deploy button takes you to the Review/Deploy Configuration page.

Related Documentation

- [Modifying Device Configuration Overview on page 53](#)

Saving the Configuration Created using the Configuration Guides

You can access Configuration Guides from the Devices workspace in Junos Space Network Management Platform. You can save the configuration on Junos Space Network Management Platform..

To save the device configuration created using the Configuration Guides:

1. Select **Network Management Platform > Devices > Device Management**.
2. Select the device for which you want to use Configuration Guides.
3. Right-click the device and select **Device Configuration > Modify Configuration**.

The Modify Configuration page is displayed. This page lists the Configuration Guides deployed with the hot-plugged application. You can also open the generic configuration editor by clicking the Schema-based Configuration Editor link.

4. Use the Configuration Guides to modify the device configuration.
5. Click **Save**.

Related Documentation

- [Configuration Guides Overview on page 63](#)

Deploying the Configuration Created using the Configuration Guides

You can access Configuration Guides from the Devices workspace in Junos Space Network Management Platform. You can deploy the configuration on the devices.

To deploy the device configuration using the Configuration Guides:

1. Select **Network Management Platform > Devices > Device Management**.
2. Select the device for which you want to use Configuration Guides.
3. Right-click the device and select **Device Configuration > View/Edit Configuration**.

The View/Edit Configuration page is displayed. This page lists the Configuration Guides deployed with the hot-plugged application. You can also open the generic configuration editor by clicking the Schema-based Configuration Editor link.

4. Use the Configuration Guides to modify the device configuration.
5. Click **Deploy**.

The Deploy Options page is displayed.

6. Select the appropriate deployment schedule from the **Date** and **Time** options.
7. Click **Deploy**.

Related Documentation

- [Configuration Guides Overview on page 63](#)

Previewing the Configuration Created using the Configuration Guides

You can access Configuration Guides from the Devices workspace in Junos Space Network Management Platform. You can preview the configuration before deploying it to the devices.

To preview the device configuration created using the Configuration Guides:

1. Select **Network Management Platform > Devices > Device Management**.
2. Select the device for which you want to use the Configuration Wizard.
3. Right-click the device and select **Device Configuration > Modify Configuration**.

The Modify Configuration page is displayed. This page lists the Configuration Guides deployed with the hot-plugged application. You can also open the generic configuration editor by clicking the Schema-based Configuration Editor link.

4. Use the Configuration Guides to modify the device configuration.
5. Click **Preview**.

The View Configuration Change page is displayed. You can view the configuration changes either in the CLI or XML formats.

6. Click **Close**.

- Related Documentation**
- [Configuration Guides Overview on page 63](#)

Resolving Out-of-Band Configuration Changes

When Junos Space Network Management Platform is the system of record, users may make out-of-band configuration changes to network devices by manually using the device's management CLI, but there is no automatic resynchronization with the Junos Space Network Management Platform database.

By viewing the configuration change log, you can see the history and details of all device configuration changes, whether initiated from Junos Space Network Management Platform or not. You can investigate details of the changes that were made, and you can decide to accept or reject the changes. If you accept them, the Junos Space Network Management Platform database is updated to reflect the new configuration. If you reject them, the device's out-of-band configuration changes are reverted.

You can resolve changes directly from the device inventory landing page by using the action Resolve OOP Change from the Actions menu. However, the configuration change log gives more detailed information.

- [Viewing the Configuration Change Log on page 65](#)
- [Managing Configuration Changes on page 66](#)

Viewing the Configuration Change Log

To view configuration changes:

1. Select **Devices > Device Management**.
The Devices inventory landing page is displayed.
2. Select the device whose configuration log you want to see.
3. Select **Device Configuration > View Configuration Change Log** from the Actions menu.
The configuration change log is displayed. [Table 14 on page 65](#) describes its contents.

Table 14: Configuration Change Log

Timestamp	The date and time at which the configuration change was made.
Author	The user ID of the person who made the change. For an in-band change, this is the Junos Space username; for an out-of-band change, it is the credential used to log into the CLI management interface.
Configuration Changes	A link to a View Configuration Change XML window in which the details of the change for this device are shown as XML.
Change Type	The type of the change: in band or out of band. Out-of-band changes are further denoted as Outstanding, Accepted, or Rejected.
Application Name	The name of the Junos Space application from which the change was requested.

Table 14: Configuration Change Log (*continued*)

Commit Comments	The commit comments included in the system log entry related to committing this change. These may include notes from the user who made the commit, as well as the timestamp and username.
-----------------	---

Managing Configuration Changes

To accept or reject configuration changes:

1. Select **Resolve outstanding out of band changes**, at the top of the Configuration Change Log window. You can also take this action directly from the devices inventory landing page by selecting Resolve OOB Changes in the Actions menu.
The Resolving OOB Changes window appears. [Table 15 on page 66](#) describes the columns in this window.

Table 15: Resolving Out-of-Band Changes

Timestamp	The date and time at which the configuration change was made.
Author	The user ID of the person who made the change. For an in-band change, this is the Junos Space username; for an out-of-band change, it is the credential used to log into the CLI management interface.
Application Name	The name of the Junos Space application from which the change was requested.
Config Change	A link to a View Configuration Change XML window in which the details of the change for this device are shown as XML.
Action	Option buttons enabling you to select Accept or Reject.

Related Documentation

- [Systems of Record in Junos Space Overview on page 733](#)

Viewing Configuration Change Log

Viewing the Configuration Change Log enables you to resolve out of band changes, which are those changes made on the device itself.

When the mode in Network Management Platform > Administration > Applications > Modify Application Settings > Device is Space as the System of Record (SSOR), the system tracks both in-band (Space) and out-of-band (non-Space) changes. When the mode in Application Settings is Network as the System of Record (NSOR) (the default), the system tracks only in-band (Space) changes.

To view the Configuration Change Log,

1. Select **Devices > Device Management**.
2. Select the device whose config change log you want to view.
3. Select **Device Configuration > View Configuration Change Log** from the Actions menu.

The View Config Change Log page appears, displaying the information listed in [Table 16 on page 67](#).

Table 16: View Configuration Change Log Table

Column Header	Explanation
Timestamp	Time when the change was committed
Author	Creator of the change
Configuration Change	Description of the change
Change Type	Type of change, that is, the workspace or tool that was used
Application Name	Name of the Junos Space application that was used
Commit Comments	Any comments made by the person committing the change.

4. To resolve any out of band changes, see [“Resolving Out-of-Band Configuration Changes” on page 65](#).

**Related
Documentation**

- [Modifying Device Configuration Overview on page 53](#)
- [Resolving Out-of-Band Configuration Changes on page 65](#)
- [Viewing Assigned Shared Objects on page 68](#)

Viewing Assigned Shared Objects

An assigned shared object is a configuration or a configuration template created for multiple devices, that is, an object that has been assigned to more than one device.

The View Assigned Shared Objects is a device-centric action that enables you to view configurations created in the applications and workspaces listed below for each device, and queue them up in preparation for publishing those changes. You can accept or reject the pending configurations, and you can change the sequence in which the changes will be committed. Accepting a configuration is assigning it, and rejecting it is unassigning it.

Configurations created by the following application workspaces can be assigned to devices:

- Network Management Platform
 - Device templates
- Security Design
 - IPSEC VPNS
 - IDP Profiles
 - Security Policies

All configurations that have been created for the device are assigned and will be candidates for deployment, unless you unassign them.

Viewing assigned shared objects can only be done on a per-device basis.

You can select only one device at a time. To view assigned shared objects:

1. Select **Devices > Device Management**.

The Device Management page appears.

2. Select the device whose assigned objects you want to view, and either
 - Select **Device Configuration > View/Assign Shared Objects** from the Actions dropdown.

The View/Assign Shared Objects page appears, listing the running configuration and the pending configurations on the right and displaying the workspaces where they originated on the left.

The pending configurations are shown in a table, whose data is described in [Table 17 on page 68](#).

Table 17: View Assigned Shared Objects Table

Column Heading	Content
Name	Name of the configuration, assigned at time of creation

Table 17: View Assigned Shared Objects Table (*continued*)

Column Heading	Content
Published	Yes or No. Templates cannot be deployed unless they are published. You can go to the Configuration Templates workspace to publish a template by clicking Configuration Templates on the panel to the left of the table.
Status	Deployed or Not Deployed
Modified By	Name of person who last modified the configuration
Modify Time	Expressed as a date (year-month-day), followed by a time (hours:minutes:seconds) and a timezone.
Description	Text entered in the Description field when the configuration was created.

All of the columns in the table have filtering enabled. Each of the configurations listed can be selected and all of the following can be performed:

- Assign Templates
- Unassign Templates
- Move Up / Move Down

From this page, you can also navigate back to the application where a configuration was created.

To assign a template:

1. On the left side of the page, select the workspace where the configuration was created.
The table on the right displays the configurations created in the selected workspace.
2. Select the check box for the configuration you want to assign, and click the [+] sign.
The template is assigned.
3. Finish by clicking **Save Changes** or **Save & Publish Changes**.

To unassign a template:

1. On the left side of the page, select the workspace where the configuration was created.
The table on the right displays the configurations created in the selected workspace.
2. Select the check box for the configuration you want to unassign, and click the [-] sign.
A Confirm dialog appears, asking you whether you want to unassign the selected object.
3. Click **Yes** to dismiss the dialog.
The template disappears from the table.
4. Finish by clicking **Save Changes** or **Save & Publish Changes**.

To change the sequence of objects, assigned or otherwise,

1. Select the check box for the configuration whose position you want to change, and click the up or the down arrow.

The object moves up or down in the display as required.

2. (Optional) Continue moving objects the same way until you are satisfied.
3. Finish by clicking **Save Changes** or **Save & Publish Changes**.

Related Documentation • [Modifying the Configuration on the Device on page 55](#)

Viewing Template Deployment (Devices)

Viewing template deployment from the Devices workspace enables you to view which templates are deployed on a device, the version of the template deployed on the device, and find out whether the device was in sync with the template at the time the last audit was performed, as well as other relevant details.

To get this information, you must perform an audit at least once after deploying a template. To ensure the information presented to you is current, perform a template configuration audit immediately before viewing template deployment. If there are any differences between template and device since the template was deployed.

To view the list of templates deployed on a device:

1. Select **Devices > Device Management**.

Device Management page lists all the devices.

2. Select the device and select **View Template Deployment** from the Actions menu.

The View Deployment page appears. lists the devices on which the template is deployed. Each device displayed in the table includes details of the device. The details include the name of the device, IP address of the device, version of the template, time when the template was deployed to the device, Junos Space user who deployed the template, job ID for deployment, template audit status, and the time when the template was audited.

Column Header	Description
Name	Name of the template that is deployed to the device.
Template Version	Version of the template currently deployed to the device.
Deploy Time	Time at which the template was deployed to the device named in this row.
Deployed By	Login ID of the person who deployed the template to the device named in this row.
Job ID	ID of the job constituted by deployment of this template to the device named in this row.

Audit Status	Unavailable, in sync or not in sync.
Audit Time	Time at which the template was deployed to the device named in this row.

3. To view the details of the template that is deployed to the device, double-click on the template name.

The Template Details window appears.

4. To view the change summary represented by a template version, click the number of the template version.

The Template Change Summary window appears, showing the configuration options that were changed due to the configuration snippet being deployed to the device.

5. To view the status of the job represented by deployment of the template, click the job ID.

The Job Management window appears.

6. To view any differences between a template and the configuration on the devices to which it has been deployed, first ensure an audit has been performed on the template since it was deployed (see [“Auditing Template Configuration” on page 219](#)).



NOTE: To view current information, audit the template configuration immediately before doing this: see [“Auditing Template Configuration” on page 219](#).



NOTE: Each audit is performed as a job. It may take some time to finish auditing, if a large number of devices were selected for auditing.

The possible states for a template audit are displayed in the Audit Status column:

- **Insync**
- **Out of sync**
- **Unavailable**—The Unavailable status is when no audit is performed on a device for a particular template. See [“Auditing Template Configuration” on page 219](#).

To view the audit status, click the link for the device in the Audit Status column.

The Template Audit Result window appears.

Under the Audit Status heading, any differences found last time the template was audited are listed. Such differences will be due to someone having altered the device configuration between the two template deployments.

7. To return to the Device Management page from the View Deployment page, click **Cancel**.

- Related Documentation**
- [Modifying Device Configuration Overview on page 53](#)

CHAPTER 5

Device Inventory

- [Viewing Physical Inventory on page 73](#)
- [Displaying Service Contract and EOL Data in the Physical Inventory Table on page 75](#)
- [Viewing Physical Interfaces on page 76](#)
- [Viewing Logical Interfaces on page 77](#)
- [Viewing and Exporting License Inventory on page 80](#)
- [Viewing and Exporting Software Inventory on page 84](#)
- [Exporting Physical Inventory Information on page 86](#)
- [Viewing Associated Scripts on page 87](#)
- [Executing Scripts on a Physical Inventory Component on page 87](#)
- [Executing Scripts on a Physical Interface on page 88](#)
- [Executing Scripts on a Logical Interface on page 89](#)
- [Applying CLI Configlets to a Physical Inventory Element on page 90](#)
- [Applying CLI Configlets to a Physical Interface on page 90](#)
- [Applying CLI Configlets to a Logical Interface on page 91](#)

Viewing Physical Inventory

Hardware inventory information shows the slots that are available for a device and provides information about power supplies, chassis cards, fans, part numbers, and so forth. Junos Space Network Management Platform displays hardware inventory by device name, based on data retrieved both from the device during discovery and resync operations, and from the data stored in the hardware catalog. For each managed device, the Junos Space Network Management Platform hardware catalog provides descriptions for field replaceable units (FRUs), part numbers, model numbers, and the pluggable locations from which empty slots are determined.

Sorting is disabled for the hardware inventory page to preserve the natural slot order of the devices.

To view hardware inventory for devices that Junos Space Network Management Platform manages:

1. **Select Devices > Device Management.**
The Device Management inventory page displays the devices managed in Junos Space Network Management Platform in a table.
2. Select a device whose inventory you want to display.
3. Select **Device Inventory > View Physical Inventory** from the Actions menu.
The inventory is displayed in a table.

You can expand certain categories (for example, the Routing Engine category) to show data for all memory (RAM and disk) installed on device components.

In the table, the address group sub types, namely, location and ship-to-address of a device will be displayed as columns only if Service Now contains address Group and is associated with devices. If no address group is configured in Service Now, then these columns will not be displayed.

The Status field on the Physical Inventory page displays the status of the device component. The status is updated during periodic re-synchronization and on notification. The different status indicators are Green (device component is present and online), Red (device component is present and offline), and Gray (device component status is unknown).

Chassis cluster devices shows information for both the primary and secondary device.

The device inventory for a Junos Space Network Management Platform installation that includes Service Now and Service Insight includes columns related to service contracts and end-of-life status. For detailed information, see [“Displaying Service Contract and EOL Data in the Physical Inventory Table” on page 75](#).

4. (Optional) Click **Export** at the top of the inventory page to export the table in CSV format. See [“Exporting Physical Inventory Information” on page 86](#).
5. Click **Return to Inventory View** to return to the device inventory page.

Related Documentation

- [Displaying Service Contract and EOL Data in the Physical Inventory Table on page 75](#)
- [Exporting Physical Inventory Information on page 86](#)
- [Viewing Managed Devices on page 41](#)
- [Viewing Physical Interfaces on page 76](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Exporting License Inventory on page 80](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)

Displaying Service Contract and EOL Data in the Physical Inventory Table

Problem **Description:** As of Release 11.3 of Junos Space, the Physical Inventory table can include columns related to the part's service contract and end-of-life (EOL) status. The service contract data in this table is populated by the Service Now Devices table. The EOL data in this table is populated by the Service Insight Exposure Analyzer table. If Service Now or Service Insight is not installed, or if the required tables are empty, these columns are not displayed in the Physical Inventory table.

Solution To investigate missing service contract and EOL data:

1. Use the table column display filters to check whether the columns have been hidden.
Select the columns you want. If the columns cannot be selected (are not listed), check your Service Now and Service Insight settings.
2. Check the Service Now Devices table for details about the devices managed with Junos Space Network Management Platform, including information about the service contract.

If you are unable to view service contract information, check the Service Now settings to ensure the following items have been properly configured:

- Service Now Organization. See Organizations Overview topic in the Service Now documentation.
 - Service Now Device. See Service Now Devices Overview topic in the Service Now documentation.
 - Service Now Device Group. See Associating Devices with a Device Group topic in the Service Now documentation.
 - Service Now Event Profile. See Event Profiles Overview topic in the Service Now documentation.
3. Check the Service Insight Exposure Analyzer table for details about the devices managed with Junos Space Network Management Platform, including information about EOL announcements.

The EOL Status column indicates whether EOL data is available or not. EOL data is available only if there is an EOL bulletin. EOL data is typically unavailable for newer products. If the Exposure Analyzer table does not contain records, there might be a problem with the Service Now configuration. Service Now manages the communication between Junos Space Network Management Platform and the Juniper Networks support organization, which is the originating source of EOL data. If the Service Insight Exposure Analyzer table is empty, check the following Service Now settings:

- Service Now Organization. See the Organizations Overview topic in the Service Now documentation.
- Service Now Device. See the Service Now Devices Overview topic in the Service Insight documentation.

Related Documentation • [Viewing Physical Inventory on page 73](#)

Viewing Physical Interfaces

Junos Space Network Management Platform displays physical interfaces by device name, based on the device information in its database. You can view the operational status and administrative status of physical interfaces for one or more devices to troubleshoot problems.

Sorting is disabled for the physical interfaces view to preserve the natural slot order of the devices.

If the interface status changes on the managed device, the information is not updated in Junos Space Network Management Platform until the device is resynchronized with the Junos Space Network Management Platform database.

You can access the Physical Interfaces view either from the Manage Devices inventory page, or from within the Physical Inventory page.

To view the physical interfaces for devices from the Manage Devices inventory page:

1. Select **Devices > Device Management**.
2. Select the device for which you want to view the physical interfaces.
3. Select **Device Inventory > View Physical Interfaces** from the Actions menu.

Junos Space Network Management Platform displays a table containing the status of the physical interfaces for the device. [Table 18 on page 76](#) describes the information that can be displayed for the physical Interfaces. Some columns may be hidden. To expose them, mouse over any column head, click the down arrow that appears, select **Columns** from the resulting menu, and check the columns you want to see.

Table 18: Physical Interfaces Columns

Field	Description
Device Name	The device configuration name.
Physical Interface Name	Standard information about the interface, in the format <i>type-/fpc/pic/port</i> , where <i>type</i> is the media type that identifies the network device; for example, ge-0/0/6.
IP Address	The IP address for the interface.
Logical Interfaces	A link to the table of logical interfaces for the device.
MAC Address	The MAC address of the device.
Operational Status	The operational status of the interface: up or down.
Admin Status	The admin status of the interface: up or down.

Table 18: Physical Interfaces Columns (*continued*)

Field	Description
Encapsulation	The encapsulation type used on the physical interface.
Link Type	The physical interface link type: full duplex or half duplex.
Speed (Mbps)	The speed at which the interface is running.
MTU	The maximum transmission unit size on the physical interface.
Description	An optional description for this interface configured on the device. It can be any text string of 512 or fewer characters. Any longer string is truncated to 512. If there is no information, the column entry is blank.

4. Click **Return to Inventory View** at the top of the inventory page.

To view the physical interfaces from physical inventory page:

1. Select **Devices > Device Management**.
2. Select the device that has the physical inventory of interest.
3. Select **Device Inventory > View Physical Inventory** from the Actions menu.

A tree grid is displayed with all the physical inventory elements of the device.

4. From the tree grid of the physical inventory, right click the component and select **View Physical Interfaces**.

Junos Space Network Management Platform displays a table containing the status of the physical interfaces for the device. [Table 18 on page 76](#) describes the information that can be displayed for the physical Interfaces. Some columns may be hidden. To expose them, mouse over any column head, click the down arrow that appears, select **Columns** from the resulting menu, and check the columns you want to see.

5. Select **Return to Physical Inventory** at the top left of the display

Related Documentation

- [Viewing Managed Devices on page 41](#)
- [Viewing Physical Inventory on page 73](#)
- [Exporting License Inventory on page 80](#)
- [Viewing Logical Interfaces on page 77](#)

Viewing Logical Interfaces

You can view logical interfaces on a per-port basis or on a per-device or per-logical system basis. You can view the logical interface configurations for one or more devices or logical systems to troubleshoot problems.

You can access the Logical Interfaces view in either of two ways: from the Manage Devices inventory page, or from within the Physical Interfaces view. These two procedures are described separately below.

To view the logical interfaces configured for a selected device from the Manage Devices inventory page:

1. Select **Devices > Device Management**.
A tabular list of devices appears.
2. Select the device for which you want to view logical interface information.
3. Do one of the following:
 - Select the **View** link in the Logical Interfaces column.
 - Select **Device Inventory > View Logical Interfaces**.
 - Right-click the selected device in the table and select **View Logical Interfaces** from the menu that appears.

Junos Space Network Management Platform displays the status of the logical interfaces for the selected device in a table. Its possible fields are described in [Table 19 on page 79](#). Some columns may be hidden. To expose them, mouse over any column head, click the down arrow that appears, select **Columns** from the resulting menu, and check the columns you want to see.

4. Select **Return to Inventory View** at the top left of the display.

To view the logical interfaces configured for a physical interface from the Physical Interfaces view:

1. Select **Devices > Device Management**.
The device inventory table appears.
2. Find the device that has the physical interfaces of interest.
3. In the table row for the device, select the word **View** in the Interfaces column.
Junos Space Network Management Platform opens a table that shows all of the physical interfaces for the device.
4. From the table of physical interfaces, find the interface for which you want to view the logical interfaces.
5. In the table row for the physical interface, select the word **View** in the Logical Interfaces column.

Junos Space Network Management Platform displays the status of the logical interfaces for the selected physical interface. Its fields are described in [Table 19 on page 79](#). Some columns may be hidden. To expose them, mouse over any column head, click the down arrow that appears, select **Columns** from the resulting menu, and check the columns you want to see.

6. Select **Return to Physical Interfaces** at the top left of the display.

Table 19: Logical Interfaces Columns

Field	Description
Device Name	The device configuration name.
Interface Name	Standard information about the interface, in the format <i>type-/fpc/pic/port/logical interface</i> , where <i>type</i> is the media type that identifies the network device; for example, ge-0/0/6.135.
IP Address	The IP address for the logical interface.
Encapsulation	The encapsulation type used on the logical interface.
Vlan	The VLAN ID for the logical interface.
Description	An optional description configured for the interface. It can be any text string of 512 or fewer characters. Any longer string is truncated. If there is no information, the column entry is blank.

Related Documentation

- [Viewing Physical Interfaces on page 76](#)

Viewing and Exporting License Inventory

The Device Licence Inventory feature enables you to display the currently installed license inventory information for all DMI schema-based devices under Junos Space Network Management Platform management.

The license inventory is generated when the device is first discovered and synchronized in Junos Space Network Management Platform.

The licenses used by all Juniper Networks devices are based on SKUs, which represent lists of features. Each license includes a list of features that the license enables and information about those features. Sometimes the license information also includes the inventory keys of hardware or software elements upon which the license can be installed.



NOTE: To view the license(s) for Junos Space Network Management Platform itself, see [“Viewing Licenses” on page 619](#).

This topic also covers:

- Absence of license
- Trial information
- Count-down information
- Date-based information

DMI enables each device family to maintain its own license catalog in the DMI Update Repository. The license catalog is a flat list of all the licenses used by a device family. The key for a license element is its SKU name. Each license element in the catalog includes a list of features that the license enables and information about each feature (that is, its name and value). Optionally, the license element can also list the inventory keys of hardware or software elements and where it can be installed.

If the license inventory on the device is changed, the result depends on whether the network is the system of record or Junos Space Network Management Platform is the system of record. See [“Systems of Record in Junos Space Overview” on page 733](#).

If the network is the system of record, Junos Space Network Management Platform automatically synchronizes with the managed device. You can also manually resynchronize the Junos Space Network Management Platform license database with the device by using the Resynchronize with Network action. See [“Resynchronizing Managed Devices With the Network” on page 94](#).

If Junos Space Network Management Platform is the system of record, neither automatic nor manual resynchronization is available.

Viewing device license inventory does not include pushing license keys to devices. You can, however, push licenses with the Configuration Editor to any device that has license keys in its configuration. See [“Modifying Device Configuration Overview” on page 53](#). You can export device license inventory information to a CSV file for use in other applications.

License inventory information shows individually installed licenses as well as a license usage summary, with statistics for various features.

To view license inventory for a device:

1. Select **Devices > Device Management**.

The Device Management inventory page displays the devices managed in Junos Space Network Management Platform.

2. Select **Device Inventory > View License Inventory** from the Actions menu.

The License Inventory page displays the license information listed in [Table 20 on page 82](#).



NOTE: Need Counts in red indicate violations. In other words, entries in red indicate that you are using features that you are not licensed to use. You may also encounter the message that you have no licenses installed.

3. (Optional) View the list of licensed features for the selected license by double-clicking a license usage summary or clicking on the forward action icon to the left of a license usage summary.

The information displayed is described in [Table 21 on page 83](#).

4. (Optional) Click **Return to Inventory View** at the top of the inventory page.

5. (Optional) Click **Export** at the top of the inventory page, to export the license inventory information.

The Export Device License Information dialog box appears, displaying a link: Download license file for selected device (CSV format).

6. (Optional) Click the download link.

The Opening Device License-xxxxxxCSV dialog box appears, where xxxxxx represents a number.

7. Open the file with an application of your choice, or download the file by clicking **Save**.

The CSV file contains the fields described in [Table 21 on page 83](#) and [Table 22 on page 83](#). These fields are not populated if the information is not available for the selected license.



NOTE: Exporting device license information generates an audit log entry.

Table 20: License Usage Summary Fields

Field	Description
Feature name	Name of the licensed SKU or feature. It can be used to look up the license with Juniper Networks. Not all devices support this.
License count	Number of times an item has been licensed. This value may have contributions from more than one licensed SKU or feature. Alternatively, it may be 1, no matter how many times it has been licensed.

Table 20: License Usage Summary Fields (*continued*)

Field	Description
Used count	Number of times the feature is used. For some types of licenses, the license count will be 1, no matter how many times it is used. For capacity-based licensable items, if infringement is supported, the license count may exceed the given count, which has a corresponding effect on the need count.
Need count	Number of times the feature is used without a license. Not all devices can provide this information.
Given count	Number of instances of the feature that are provided by default.

Table 21: License Feature or SKU Fields

Field	Description
Feature Name	Name of the licensed SKU or feature. It can be used to look up the license with Juniper Networks. Not all devices support this.
Validity Type	The SKU or feature is considered permanent if it is not trial, count-down, or data-based.

Table 22: Additional Fields in CSV Files

Field	Description
State	Status of the license: valid, invalid, or expired. Only licenses marked as valid are considered when calculating the license count.
Version	
Type	Permanent, trial, and so on.
Start Date	Licensed feature starting date.
End Date	Licensed feature ending date.
Time Remaining	Licensed feature time remaining.

**Related
Documentation**

- [Viewing Managed Devices on page 41](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Systems of Record in Junos Space Overview on page 733](#)

Viewing and Exporting Software Inventory

The Device Software Inventory feature enables you to display the currently installed software inventory information for all DMI schema-based devices under Junos Space Network Management Platform management.

The software inventory is generated when the device is first discovered and synchronized in Junos Space Network Management Platform. If the software inventory on the device is changed by a local user, the result depends on whether the network is the system of record or Junos Space Network Management Platform is the system of record. See [“Systems of Record in Junos Space Overview” on page 733](#).

If the network is the system of record, Junos Space Network Management Platform automatically synchronizes with the managed device. You can also manually resynchronize the Junos Space Network Management Platform software database with the device by using the Resynchronize with Network action. See [“Resynchronizing Managed Devices With the Network” on page 94](#).

If Junos Space Network Management Platform is the system of record, neither automatic nor manual resynchronization is available. You can reset the device configuration from the values in the Junos Space Network Management Platform database if and when you want to do so.

If you need to install software on a device, see [“Modifying Device Configuration Overview” on page 53](#). You can export device software inventory information to a CSV file for use in other applications (steps 5 through 7).

To view software inventory for a device:

1. Select **Devices > Device Management**.

The Device Management inventory page displays the devices managed in Junos Space Network Management Platform.

2. Select a device or devices by clicking the boxes next to their names, and then select **Device Inventory > View Software Inventory** from the Actions menu. You can sort the device column either by clicking the arrow in the column head or by mousing over the column head and clicking your choice of Sort Ascending or Sort Descending.

If you selected more than one device, the report is grouped by device name. You can expand or contract each section by clicking the icon to the left of each device name.

3. (Optional) You can control which columns are displayed by mousing over any column head and clicking Columns in the drop-down menu, then checking the column names that you want. The Version column is redundant with the Major, Minor, and Revision columns. You might need only one or two of these.
4. (Optional) Click **Return to Inventory View** at the top of the software inventory page.
5. (Optional) Click **Export**, at the top of the inventory page, to export the software inventory information.

The Export Software Inventory dialog box appears, displaying a link: Download software inventory for selected device (CSV format).

6. (Optional) Click the download link.
7. Open the file with an application of your choice, or download the file by clicking **Save**. You can designate a filename and location.

The CSV file contains the following fields: Device Name, Product Model, Package Name, Version, Type, and Description, as detailed in [Table 23 on page 85](#), irrespective of the columns you have chosen to display on the screen. These fields are not populated if the information is not available for the selected software.

Table 23: Software Inventory Fields

Field	Description
Device	Name of the device on which this software inventory is present.
Model	The model of this device. Possible device families include J Series, M Series, MX Series, TX Series, SRX Series, EX Series, BXOS Series, and QFX Series.
Routing engine	On a device supporting multiple Routing Engines, indicates which Routing Engine is described.
Package name	Name of the installed software package.
Description	Description of the installed software package.
Version	Version number of the installed software package.
Type	Type of the installed software package. Permitted values are operating-system, internal-package, and extension.
Major	Major portion of the version number. For example, in version 11.4R1.14, the major portion is 11.
Minor	Minor portion of the version number. For example, in version 11.4R1.14, the minor portion is 4.
Revision number	The revision number of the package. For example, in version 11.4R1.14, the revision number is 1.14.

Related Documentation

- [Viewing Managed Devices on page 41](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Systems of Record in Junos Space Overview on page 733](#)
- [Device Images and Scripts Overview on page 269](#)

Exporting Physical Inventory Information

You can view the list of devices managed through Junos Space Network Management Platform and export the device information to a comma-separated value (CSV) file from the Devices workspace. You can import this CSV file into other applications, such as those you use for asset management. The export task runs as a Junos Space Network Management Platform job.

You can view the device inventory summary in a tabular format from the Device Management task in the task tree.

To export the device inventory summary:

1. Display the device inventory by selecting **Devices > Device Management**.

The Device Management table appears.

2. Select the devices you want to include in the device inventory report.
3. (Optional) To preview the device information before you export to the CSV file, select **Device Inventory > View Physical Inventory** from the Actions menu.

The physical inventory page appears.

You can expand the information in this view to see the details of each device. Click the plus sign (+) to the left of the device in the list.

If you want to change the content of the report, select the **Return to Inventory View** link in the top-left corner to display the device summary table again. You can make a new selection or continue with the export.

4. Select **Device Inventory > Export Physical Inventory** from the Actions menu to create the CSV file.

The Export Inventory dialog box appears.

5. Click either the **Export Selected** button or the **Export All** button to begin creating the CSV file.

Clicking an export button starts a Junos Space Network Management Platform job that creates and saves the CSV report. When the job is completed, the Export Inventory Job Status report indicates the job is 100% complete.

6. Click the **Download** link in the Export Inventory Job Status report to download the CSV file.

The CSV file you have downloaded displays the physical inventory details such as the name of the device, chassis, name of the module, name of the sub module, name of the sub sub module, name of the sub sub sub module, model number of the device, model of the device, part number of the device, revision number of the device, serial number of the device, and the description provided for the device.

You can import this CSV file into other applications, such as those you might use for asset management.

- Related Documentation**
- [Device Inventory Overview on page 40](#)
 - [Viewing Managed Devices on page 41](#)
 - [Junos Space User Interface Overview on page 9](#)
 - [Viewing Physical Inventory on page 73](#)
 - [Device Management Overview on page 35](#)
 - [Device Discovery Overview on page 131](#)

Viewing Associated Scripts

To view the scripts associated with the devices:

1. Select **Devices > Device Management**.
The Device Management page is displayed.
2. Select the devices for which you want to view the associated scripts.
3. Select **Device Inventory > View Associated Scripts** from the Actions menu.

The View Associated Scripts page is displayed. This page displays all the scripts that are deployed on the devices you have selected. You can view the script name, script type, staged version of the script, latest version of the script, and the activation status of the script.

- Related Documentation**
- [Device Inventory Overview on page 40](#)

Executing Scripts on a Physical Inventory Component

To execute scripts on a physical inventory component of the device:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Inventory > View Physical Inventory**.
4. Right click the physical inventory component of interest and select **Execute Script**.

The Execute Script page displays the scripts that are associated and enabled on the selected device. The context of the script also matches with the context of the selected physical inventory component of the device.

5. Select the script that you want to execute on the physical inventory component of the device.

You can click the **View Context** link to view the context of the selected physical inventory component of the device.

6. Enter the values for the parameters.

7. To schedule a time for executing scripts on the physical inventory component of the device, select the **Schedule at a later time** check box and specify the date and time when you want the script to be executed.
8. Click **Execute**.

The Script Execution Job Results window displays the following information - Device name, Entity name, Script Execution status and Script Execution Results. The result HTML is processed and rendered to allow you to read and understand the Script Execution Results. A progress bar indicates the status of Script Execution Job.



NOTE: If you schedule the Script Execution Job for a later point in time, the Script Execution Job Results window does not appear. Instead the Job dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page.

You can double click the task to view the Script Management Job status window. Clicking the View results link in the Description column displays the results of Script Execution. Here the result HTML is processed and rendered to allow you to read and understand the Script Execution Results.

Related Documentation • [Applying CLI Configlets to the Physical Inventory on page 90](#)

Executing Scripts on a Physical Interface

To execute scripts on a physical interface of the device:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Inventory > > View Physical Interfaces**.
4. Right click the physical interface of interest and select **Execute Script**.

The Execute Script page displays the scripts that are associated and enabled on the selected device. The context of the script also matches with the context of the selected physical interface of the device.

5. Select the script that you want to execute on the physical interface of the device.

You can click the **View Context** link to view the context of the selected physical interface of the device.

6. Enter the values for the parameters.
7. To schedule a time for executing scripts on the physical interface of the device, select the **Schedule at a later time** check box and specify the date and time when you want the script to be executed.
8. Click **Execute**.

The Script Execution Job Results window displays the following information - Device name, Entity name, Script Execution status and Script Execution Results. The result HTML is processed and rendered to allow you to read and understand the Script Execution Results. A progress bar indicates the status of Script Execution Job.



NOTE: If you schedule the Script Execution Job for a later point in time, the Script Execution Job Results window does not appear. Instead the Job dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page.

You can double click the task to view the Script Management Job status window. Clicking the View results link in the Description column displays the results of Script Execution. Here the result HTML is processed and rendered to allow you to read and understand the Script Execution Results.

Related •
Documentation

Executing Scripts on a Logical Interface

To execute scripts on a logical interface of the device:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Inventory > > View Physical Interfaces**.
4. Right click the logical interface of interest and select **Execute Script**.

The Execute Script page displays the scripts that are associated and enabled on the selected device. The context of the script also matches with the context of the selected logical interface of the device.

5. Select the script that you want to execute on the logical interface of the device.

You can click the **View Context** link to view the context of the selected logical interface of the device.

6. Enter the values for the parameters.
7. To schedule a time for executing scripts on the logical interface of the device, select the **Schedule at a later time** check box and specify the date and time when you want the script to be executed.
8. Click **Execute**.

The Script Execution Job Results window displays the following information - Device name, Entity name, Script Execution status and Script Execution Results. The result HTML is processed and rendered to allow you to read and understand the Script Execution Results. A progress bar indicates the status of Script Execution Job.



NOTE: If you schedule the Script Execution Job for a later point in time, the Script Execution Job Results window does not appear. Instead the Job dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page.

You can double click the task to view the Script Management Job status window. Clicking the View results link in the Description column displays the results of Script Execution. Here the result HTML is processed and rendered to allow you to read and understand the Script Execution Results.

Related •
Documentation

Applying CLI Configlets to a Physical Inventory Element

To apply a CLI configlet to a physical inventory element on a device:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Inventory > View Physical Inventory**.
4. Right click the physical inventory element for which the CLI configlet has to be applied
5. Select **Apply CLI Configlets**.

The Apply CLI Configlet page displays the list of CLI configlets that match the context of the selected physical inventory element.

6. Select the CLI configlet to be applied and enter the value for parameters if required.
7. Click **Apply** (On the second step of the wizard if preview is enabled).

Related •
Documentation

Applying CLI Configlets to a Physical Interface

To apply a CLI configlet to a physical interface of a device:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Inventory > View Physical Interfaces**.
4. Right click the physical interface for which the CLI configlet has to be applied
5. Select **Apply CLI Configlets**.

The Apply CLI Configlet page displays the list of CLI configlets that match the context of the selected physical interface.

6. Select the CLI configlet to be applied and enter the value for parameters if required.
7. Click **Apply** (On the second step of the wizard if preview is enabled).

Related •
Documentation

Applying CLI Configlets to a Logical Interface

To apply a CLI configlet to a logical interface of a device:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Inventory > View Logical Interfaces**.
4. Right click the logical interface for which the CLI configlet has to be applied
5. Select **Apply CLI Configlets**.

The Apply CLI Configlet page displays the list of CLI configlets that match the context of the selected logical interface.

6. Select the CLI configlet to be applied and enter the value for parameters if required.
7. Click **Apply** (On the second step of the wizard if preview is enabled).

Related •
Documentation

CHAPTER 6

Device Operations

- [Deleting Devices on page 93](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Using Looking Glass on page 96](#)
- [Understanding Logical Systems for SRX Series Services Gateways on page 97](#)
- [Creating a Logical System \(LSYS\) on page 98](#)
- [Deleting Logical Systems on page 99](#)
- [Viewing the Physical Device for a Logical System on page 99](#)
- [Viewing Logical Systems for a Physical Device on page 100](#)
- [Putting a Device in RMA State and Reactivating Its Replacement on page 101](#)
- [Applying CLI Configlets to a Device on page 103](#)
- [Executing Scripts on Devices on page 103](#)
- [Executing Scripts on Devices Remotely with JUISE on page 104](#)

Deleting Devices

You can delete devices from Junos Space Network Management Platform. Deleting a device removes all device configuration and device inventory information from the Junos Space Network Management Platform database.

To delete a device from Junos Space Network Management Platform:

1. Select **Devices > Device Management**.

Graphical summaries about the devices in the network appear.

2. Expand the Devices workspace by clicking the expansion symbol to the left of its name.

Tasks related to managing devices are displayed in the expanded portion of the tree. Some (for example, Discover Devices) can be further expanded.

3. From the task tree, select **Device Management**.

The Device Management inventory page displays information about the devices managed in Junos Space Network Management Platform.

4. (Optional) View summary information for a device before deleting by selecting the device and moving the scroll bar to the far right.

Junos Space Network Management Platform displays basic device information, including name, OS version, platform, IP address, and connection status.

5. From the Device Management inventory page, select one or more devices to delete.
6. If provisioning services are associated with a device that you want to delete, you must remove the provisioning services before deleting the device. See *Deleting a Service Order*.

7. Select **Device Operations > Delete Devices** from the Actions menu.

Junos Space Network Management Platform displays the Delete Devices dialog box.

8. Select **Delete** to delete the selected devices.

Junos Space Network Management Platform deletes all device configuration and inventory information for the selected devices from the Junos Space Network Management Platform database.

**Related
Documentation**

- [Viewing Managed Devices on page 41](#)
- [Viewing Physical Inventory on page 73](#)
- [Viewing Physical Interfaces on page 76](#)
- [Discovering Devices on page 132](#)

Resynchronizing Managed Devices With the Network

If the network is the system of record, you can resynchronize a managed device at any time. For example, when a managed device is updated by a device administrator from the device's native GUI or CLI, you can resynchronize the device configuration in the Junos Space Network Management Platform database with the physical device. (If Junos Space Network Management Platform is the system of record, this capability is not available. See [“Systems of Record in Junos Space Overview” on page 733.](#))

To resynchronize a device:

1. Select **Devices > Device Management** workspace.
2. Expand the Devices workspace by clicking the expansion symbol to the left of its name.

Tasks related to managing devices are displayed in the expanded portion of the tree. Some (for example, Discover Devices) can be further expanded.

3. Select **Device Management**.

The Device Management inventory page displays the list of managed devices by name and IP address.

4. From the Device Management inventory page, select one or more devices to resynchronize:

5. Select **Device Operations > Resynchronize with Network** to reimport the devices in Junos Space Network Management Platform.

Junos Space Network Management Platform displays the Resynchronize Devices dialog box.

6. Click **Confirm**.

Junos Space Network Management Platform starts resynchronizing the device and displays the Resynchronization status message, as shown in the following example.

7. Click the Job ID to view details about the device resynchronization, or click **OK** to close the message.

When a resync job is scheduled to run but another resync job on the same device is in progress, Junos Space Network Management Platform delays the scheduled resync job. The time delay is determined by the damper interval that you set from the application workspace. By default the time delay is 20 seconds. The scheduled job is delayed as long as the other resync job to the same device is in progress. When the job that is currently running finishes, the scheduled resync job starts. See [“Modifying Junos Space Application Settings” on page 624](#).

**Related
Documentation**

- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Systems of Record in Junos Space Overview on page 733](#)
- [Device Inventory Overview on page 40](#)
- [Viewing Managed Devices on page 41](#)
- [Viewing Physical Inventory on page 73](#)
- [Viewing Physical Interfaces on page 76](#)
- [Exporting License Inventory on page 80](#)

Using Looking Glass

You can check the configuration settings of one or more devices from Junos Space Network Management Platform using Looking Glass. It enables you to execute **show** commands across multiple devices to compare the configuration and runtime information.

Looking Glass supports many Junos OS **show** commands, which you can see in a drop-down list. The availability of commands depends on the device platform and the OS version. (The **show** commands supported for each device platform and Junos OS version are loaded into the database during configuration import.)

Looking Glass offers two views for the command outputs—text output and table view. Text output simulates the CLI, whereas table view resembles the information display on the Devices page in Junos Space Network Management Platform.

Although Looking Glass is available for most devices, not every user can manage all devices. Permissions to use Looking Glass must be assigned as part of a user's role. Without permissions to manage a device, you cannot use Looking Glass on it.



NOTE: Looking Glass does not support ScreenOS or logical systems.

To run a **show** command from Junos Space Network Management Platform:

1. From the task tree, select **Devices > Device Management**.

The Device Management inventory page displays the devices managed in Junos Space Network Management Platform.

2. Select **Device Operations > Looking Glass** from the Actions menu.

The Looking Glass page appears, displaying the name of the device(s) selected and their icons on the upper part of the page, above the Execute Command field and the Refresh Response button.

3. Begin to enter a **show** command in the **Execute Command** field.

A list of suggestions appears below the field. The suggestions are based on the commands that can be executed on the device(s) currently selected. Usually viewing the entire list requires vertical scrolling.

4. Either finish entering your command or select it from the list.

5. If the command you are running requires your input, replace the part of the command shown as text in angle brackets with your own data. For example, replace **<slot>** in **show chassis routing-engine <slot>** with the slot number, as in **show chassis routing-engine 1**.



NOTE: If you do not enter required input, there is no output in response to the **show** command.

6. Click **Refresh Response** if necessary. (If you typed an entire command without selecting from the drop-down list, you will need to do this.)

The command you entered or selected is displayed to the right of the Refresh Response button. The command output is displayed in the lower panel of the page.

Especially in table view, you should expect to scroll horizontally. With multiple devices selected, you must scroll vertically as well.

If there is no output, the lower part of the page remains blank.

All the details shown in Looking Glass are obtained directly from the devices and may not be formatted as well as those displayed on the Space inventory landing pages.

7. (Optional) To change the way the output is displayed, click the Format Text View icon in the Execute Command banner, between the View Response button and the displayed command name. The default view is Table View.
8. (Optional) To display only a single device's output on a page showing the output for multiple devices, click the device's icon in the upper part of the page.
A green check mark appears on the icon, and the lower panel of the window displays the output for the selected device only.
9. (Optional) To remove all selections, click in the empty part of the upper section of the page.
All check marks disappear, and the lower panel displays no output.
10. (Optional) To display the output for a subset of devices on a page showing the output for multiple devices, hold down the Ctrl key or the Shift key as you click the icons for the devices whose output you want to display.
Green check marks appear on the icons of the devices you select, and the lower panel of the window displays the output for the selected devices only.



TIP: If you are looking at output across multiple devices in Format Text View, use the individual vertical scrollbar at the far right of the page for each device to see the entire output. You can position the slider to show the same output parameters for different devices you are comparing.

Related Documentation

- [Viewing Managed Devices on page 41](#)
- [Viewing Physical Inventory on page 73](#)
- [Viewing Physical Interfaces on page 76](#)
- [Discovering Devices on page 132](#)

Understanding Logical Systems for SRX Series Services Gateways

Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. By transforming

an SRX Series device into a multitenant logical systems device, you can give various departments, organizations, customers, and partners—depending on your environment—private use of portions of its resources and a private view of the device. Using logical systems, you can share system and underlying physical machine resources among discrete user logical systems and the master logical system. The logical systems feature runs with the Junos operating system (Junos OS) on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

For detailed information about understanding and configuring logical systems for SRX series services gateways, see *Junos OS Logical Systems Configuration Guide for Security Devices*

**Related
Documentation**

- [Viewing Devices and Logical Systems with QuickView on page 46](#)
- [Viewing the Physical Device for a Logical System on page 99](#)
- [Viewing Logical Systems for a Physical Device on page 100](#)
- [Creating a Logical System \(LSYS\) on page 98](#)
- [Deleting Logical Systems on page 99](#)
- *Junos OS Logical Systems Configuration Guide for Security Devices*

Creating a Logical System (LSYS)

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*

To create a new logical system on a physical device:

1. Select **Devices > Device Management**.
2. Select a physical device and then select **Device Operations > Create LSYS** from the Actions menu.

The new logical system window opens, prompting you to enter information for the new logical system.

3. In the LSYS device name box, enter the name for the new logical system.
4. From the LSYS profile menu, choose a logical system security profile for the new logical system. For more information about security profiles, see *Junos OS Logical Systems Configuration Guide for Security Devices*
5. Click **Finish** to create the new logical system.

Junos Space Network Management Platform shows you the ID number of the job for creating the new logical system. You can click on the ID number to check status of the job.

**Related
Documentation**

- [Understanding Logical Systems for SRX Series Services Gateways on page 97](#)
- [Viewing Devices and Logical Systems with QuickView on page 46](#)
- [Viewing the Physical Device for a Logical System on page 99](#)

- [Viewing Logical Systems for a Physical Device on page 100](#)
- [Deleting Logical Systems on page 99](#)
- *Junos OS Logical Systems Configuration Guide for Security Devices*

Deleting Logical Systems

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*



NOTE: We recommend that you *not* delete an SRX root device and an LSYS simultaneously in Junos Space Network Management Platform. Although deleting the SRX root device will delete the root device and the LSYS instances from Junos Space Network Management Platform, it will not remove the LSYS configuration from the device, whereas deleting an LSYS will remove LSYS-related configuration from the device.

To delete one or more existing logical systems:

1. Select **Devices > Device Management**.
2. Select a logical system and then select **Device Operations > Delete Devices** from the Actions menu.

Junos Space Network Management Platform opens a dialog box prompting you to confirm the deletion of the selected logical systems.

3. Click **Confirm** to proceed with the deletion of the logical systems, or click **Cancel** to return to the Manage Devices view without deleting the logical systems.

Related Documentation

- [Understanding Logical Systems for SRX Series Services Gateways on page 97](#)
- [Viewing Devices and Logical Systems with QuickView on page 46](#)
- [Viewing the Physical Device for a Logical System on page 99](#)
- [Viewing Logical Systems for a Physical Device on page 100](#)
- [Creating a Logical System \(LSYS\) on page 98](#)
- *Junos OS Logical Systems Configuration Guide for Security Devices*

Viewing the Physical Device for a Logical System

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*

To view the physical device on which a selected logical system is configured:

1. Select **Devices > Device Management**.

2. In the tabular view, locate the table row for the logical system.

The logical system name will be followed by link text indicating the name of the physical device on which the logical system is configured.

3. Click on the link text next to the name of the logical system.

Space Platform filters the device inventory list so that it shows only the entry for the physical device on which the logical system is configured.

4. To clear the filter and return the inventory list to its original view, click the red X next to the filter criteria above the inventory list.

**Related
Documentation**

- [Understanding Logical Systems for SRX Series Services Gateways on page 97](#)
- [Viewing Devices and Logical Systems with QuickView on page 46](#)
- [Viewing Logical Systems for a Physical Device on page 100](#)
- [Creating a Logical System \(LSYS\) on page 98](#)
- [Deleting Logical Systems on page 99](#)
- *Junos OS Logical Systems Configuration Guide for Security Devices*

Viewing Logical Systems for a Physical Device

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*.

To view the logical systems configured on a selected physical device:

1. Select **Devices > Device Management**.

2. Locate the table row for the physical device.

If the device supports logical systems, the device name will be followed by link text indicating how many logical systems are configured on it. If no logical systems are configured on the device, the link text reads "0 LSYS(s)."

3. Click on the link text next to the name of the physical device.

Space Platform filters the device inventory list so that it lists the logical systems configured on the selected physical device.

4. To clear the filter and return the inventory list to its original view, click the red X next to the filter criteria above the inventory list.

**Related
Documentation**

- [Understanding Logical Systems for SRX Series Services Gateways on page 97](#)
- [Viewing Devices and Logical Systems with QuickView on page 46](#)
- [Viewing the Physical Device for a Logical System on page 99](#)

- [Creating a Logical System \(LSYS\) on page 98](#)
- [Deleting Logical Systems on page 99](#)
- *Junos OS Logical Systems Configuration Guide for Security Devices*

Putting a Device in RMA State and Reactivating Its Replacement

Sometimes, because of hardware failure, a device managed by Junos Space Network Management Platform needs to be returned to the vendor for repair or replacement. In such cases, Junos Space Network Management Platform can keep on record the configuration of the defective device until you can obtain an equivalent replacement device from the vendor. You create this record by putting the defective device in Return Materials Authorization (RMA) state before removing it. In this way, you prevent the configuration from being deleted from the Junos Space Network Management Platform database when the device is removed.

Before connecting the replacement device, you must configure it with such basic information as the name, IP address, and login credentials (which must exactly match those of the original device when it was put in RMA state).

Once the replacement device has been reconnected within your network, you perform the Reactivate from RMA task to cause Junos Space Network Management Platform to read its settings, put the preserved configuration onto it, and bring it back under management. Because the two devices are perceived as equivalent, this operation is considered reactivation, even if the replacement device is new.

Do not delete or physically disconnect the defective device before performing the Put in RMA State task.



WARNING: Remove any provisioning services associated with a device before putting it in RMA state.

- [Putting a Device in RMA State on page 101](#)
- [Reactivating a Replacement Device on page 102](#)

Putting a Device in RMA State

If you want to return a device to the vendor under RMA, but you do not want to delete its configuration from the Junos Space Network Management Platform database, put the device in RMA state.

To have Junos Space Network Management Platform keep on record the configuration of a defective device so that you can later deploy that configuration to the defective device's replacement:

1. Select **Devices > Device Management**.

The **Device Management** inventory page displays the devices managed in Junos Space Network Management Platform.

2. Select the defective device.
3. Select **Device Operations > Put in RMA State** from the Actions menu.

The RMA Device window appears.

4. Click **Confirm** to put the selected device in RMA state.

The RMA Devices Information window appears, displaying the job ID, which you can click to view details.

5. Click **OK** to return to the Device Management inventory page.

The defective device is still displayed, but it is no longer active. The Connection Status column reports that the device is down, and the Managed Status column reports that the device is In RMA.

Reactivating a Replacement Device

Before you begin, you must perform basic configuration on the replacement device, such as the name, IP address, and login credentials. These values must match those of the original device when it was put in RMA state.

To have Junos Space Network Management Platform deploy the configuration of a defective device to a replacement device:

1. Connect the replacement device to your network in the same way as the defective device was connected.

2. Select **Devices > Device Management**.

The Device Management inventory page displays the devices managed in Junos Space Network Management Platform.

3. Select the item that formerly represented the defective device. (It in fact now represents the replacement device, without the need for you to make any changes to it.)

4. Select **Device Operations > Reactivate from RMA** from the Actions menu.

5. Click **Confirm** to activate the replacement device.

The RMA Devices Information window appears, displaying the job ID, which you can click to view details.

6. Click **OK** to return to the Device Management inventory page.

The replacement device is displayed, now with the defective device's configuration.

As activation proceeds, intermediate states such as Reactivating are displayed under Managed Status. The replacement device is active and under management when Connection Status reports that the device is up, and Managed Status reports In Sync.

Applying CLI Configlets to a Device

To apply a CLI configlet to a device:

1. Select **Platform > Devices > Device Management**.
2. Right click the device of interest and select **Device Operations > Apply CLI Configlet**.

The Apply CLI Configlet page displays the list of CLI configlets that match the context of the selected device.

3. Select the CLI configlet to be applied and enter the value for parameters if required.
4. Click **Apply**.

Related Documentation

- [Executing Scripts on Devices on page 103](#)

Executing Scripts on Devices

To execute scripts on a selected device from the Manage Devices Inventory page:

1. Select **Platform > Devices > Device Management**.
2. Select the device of interest.
3. Right click the device and select **Device Operations > Execute Scripts**.

The Execute Scripts page displays the scripts that are associated and enabled on the selected device. The context of the script also matches the context of the selected device.

4. Select the script that you want to execute on the device.

You can click the **View Context** link to view the context of the selected device.

5. Enter the values for the parameters.
6. To schedule a time for executing scripts on devices, select the **Schedule at a later time** check box and specify the date and time when you want the script to be executed.
7. Click **Execute**.

The Script Execution Job Results window displays the following information - Device name, Entity name, Script Execution status and Script Execution Results. The result HTML is processed and rendered to allow you to read and understand the Script Execution Results. A progress bar indicates the status of Script Execution Job.



NOTE: If you schedule the Script Execution Job for a later point in time, the Script Execution Job Results window does not appear. Instead the Job dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page.

You can double click the task to view the Script Management Job status window. Clicking the View results link in the Description column displays the results of Script Execution. Here the result HTML is processed and rendered to allow you to read and understand the Script Execution Results.

Related Documentation • [Applying CLI Configlets to Devices on page 103](#)

Executing Scripts on Devices Remotely with JUISE

From Junos Space Release 13.1 onwards, the Junos Space image comes integrated with the Junos OS User Interface Scripting Environment (JUISE—jui-se-0.3.10-1 version) which enables you to execute a script on a remote device from the Junos Space server without having to discover the device or stage the script on the device. The only condition that should be met is that the device should be reachable from the Junos Space server.

By default, JUISE is installed when you install or upgrade to Junos Space Release 13.1. Only SLAX scripts (*.slax) can be executed using JUISE.

To execute scripts on Junos OS devices with JUISE:

1. Log on to the Junos Space server system console.
2. Type the following command:

`jui-se [[user]@target] [options] [script] [param value]`, where

- user—Username of the target device
- target—Target device on which you want to execute the script
- options—Options to customize the execution of the script
- script—Path to the script file on the Junos Space server
- param value—A set of name/value pairs that are passed as parameters to the script

For example, `jui-se --user root --target 10.1.1.1 /home/admin/show_chassis_hardware.slax`

Related Documentation • [Scripts Overview on page 275](#)

CHAPTER 7

Device Access

- [Secure Console Overview on page 105](#)
- [Connecting to a Device From Secure Console on page 106](#)
- [Launching a Device's Web UI on page 109](#)
- [Changing Device Credentials on page 110](#)
- [Key-based Authentication Overview on page 111](#)
- [Generating and Uploading Authentication Keys to Devices on page 112](#)
- [Resolving Key Conflicts on page 116](#)
- [Changing Device Authentication from Password-based to Key-based Authentication on page 116](#)

Secure Console Overview

From the Junos Space user interface, you can use the Secure Console feature to open an SSH session to connect to a Junos Space Network Management Platform managed device or unmanaged device. The Secure Console is a terminal window embedded in Junos Space Network Management Platform that eliminates the need for a third party SSH client.

Secure Console initiates the SSH session from the Junos Space server (rather than from your browser) to provide a secure and reliable connection for both managed and unmanaged devices.

You can use Secure Console to connect to any managed device in Junos Space Network Management Platform by using the credentials previously stored for the device. To connect to devices that are not managed by Junos Space Network Management Platform, you must provide device credentials before connecting to the device.

You can establish multiple SSH connections to connect to different devices simultaneously, with each SSH connection in a different window.

You must have Super Administrator or Device Manager privileges to open an SSH session to a device in Junos Space Network Management Platform.

Related Documentation

- [Connecting to a Device From Secure Console on page 106](#)

Connecting to a Device From Secure Console

You can use Secure Console to establish a connection to a device directly from the Junos Space user interface. Secure Console uses the SSH protocol to provide a secure remote access connection to a device. After you connect to a device, you can enter CLI commands from the terminal window to monitor or troubleshoot the device. You can use Secure Console to establish a connection to a managed device or unmanaged device. An unmanaged device is a device that has not been discovered in Junos Space Network Management Platform.

This topic includes the following tasks:

- [Connecting to a Managed Device from the Device Management Page on page 106](#)
- [Connecting to an Unmanaged Device from the Device Management Page on page 107](#)
- [Connecting to a Managed or Unmanaged Device from the Secure Console Page on page 108](#)

Connecting to a Managed Device from the Device Management Page

To open an SSH session to connect to a managed device, the following conditions must be met:

- You must have Super Administrator or Device Manager privileges in Junos Space Network Management Platform.
- The status of the managed device must be “UP”

You can use Secure Console to establish a connection to a Junos Space Network Management Platform managed device. Secure Console uses the SSH protocol to provide a secure remote access connection to your managed devices.

To connect to the managed device:

1. Select **Devices > Device Management**.

The Device Management inventory page displays managed devices by name and IP address.

2. Select a device by selecting the table row for the device.
3. In the Actions menu, click **Secure Console**.

A terminal window opens in a non-modal popup with the SSH connection opened on the selected device.



NOTE: You might encounter the error messages “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. When an error occurs, all other functionality in the terminal window is stopped. When you encounter such an error, you can close the terminal window and open a new SSH session.

4. From the terminal window prompt, you can enter CLI commands to monitor or troubleshoot the device.

Secure Console supports the following terminal control characters:

- **CRTL + A**—moves cursor to start of the command line
 - **CRTL + E**—moves cursor to end of the command line
 - **↑** (up arrow key)—repeats the last command
 - **TAB**—completes a partially typed command
5. To terminate the SSH session, type **exit** from the terminal window prompt and press Enter.
 6. Click in the top right corner of the terminal window to close the window.

Connecting to an Unmanaged Device from the Device Management Page

You can use Secure Console to establish a connection to an unmanaged device.

To open an SSH session to connect to an unmanaged device, the following conditions must be met:

- You must have Super Administrator or Device Manager privileges in Junos Space Network Management Platform.
- The device is configured with a static management IP address that is reachable from the Junos Space Appliance.
- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:

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

- The status of the device must be “UP”
- A valid user name and password is created on the device.

To connect to an unmanaged device:

1. From the task tree, select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the device.
3. To establish an SSH connection for the device, specify the administrator user name and password.

The name and password must match the name and password configured on the device.

4. Specify the port number.
5. Click **Connect**.

A terminal window opens in a non-modal popup with an SSH connection opened on the selected device.



NOTE: You might encounter the error messages “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. When an error occurs, all other functionality in the terminal window is stopped. If you encounter such an error, you can close the terminal window and open a new SSH session.

6. From the terminal window prompt, you can enter CLI commands to monitor or troubleshoot the device.

Secure Console supports the following terminal control characters:

- **CRTL + A**—moves cursor to start of the command line
 - **CRTL + E**—moves cursor to end of the command line
 - **↑** (up arrow key)—repeats the last command
 - **TAB**—completes a partially typed command
7. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
 8. Click in the top right corner of the terminal window to close the window.

Connecting to a Managed or Unmanaged Device from the Secure Console Page

Before you connect to a managed or unmanaged device from the Secure Console page, ensure that:

- You have the privileges of a Super Administrator or Device Manager in Junos Space Network Management Platform.
- The device is configured with a static management IP address. This IP address should be reachable from the Junos Space Appliance.
- The SSH v2 protocol is enabled on the device.

To enable SSH v2 on a device, enter the **set system services ssh protocol-version v2** command at the command prompt.

- The status of the device is “UP”.
- A valid username and password are created on the device.

To connect to a managed or unmanaged device from the Secure Console page:

1. On the Junos Space Network Management Platform user interface, select **Devices > Secure Console**.

The Secure Console page is displayed. This page displays the fields you need to specify to connect using the Secure Console.

2. In the **IP Address** field, enter a valid IP address of the device.
3. In the **Username** field, enter the username of the device.

The username must match the username configured on the device.

4. In the **Password** field, enter the password to access the device.

The password must match the password configured on the device.

5. In the **Port** field, enter the port number to use for the SSH connection.

The default value is 22. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.

6. Click **Connect**.

A terminal window opens in a non-modal popup with an SSH connection opened on the selected device.



NOTE: You might encounter the error messages “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. When an error occurs, all other functionality in the terminal window is stopped. If you encounter such an error, you can close the terminal window and open a new SSH session.

7. From the terminal window prompt, you can enter CLI commands to monitor or troubleshoot the device.

Secure Console supports the following terminal control characters:

- **CRTL + A**—moves cursor to start of the command line
- **CRTL + E**—moves cursor to end of the command line
- **↑** (up arrow key)—repeats the last command
- **TAB**—completes a partially typed command

8. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.

9. Click in the top right corner of the terminal window to close the window.

Related Documentation

- [Secure Console Overview on page 105](#)

Launching a Device's Web UI

The Launch Device WebUI action enables you to access the WebUI of a device to manage it directly. The device should have the required Web UI components installed and enabled (for example, J-web).

Once launched, the Web UI appears either in a new tab in your browser or in a new window. Ensure you enable pop-ups on your browser for the device for which the Web UI is being launched.

To launch a device Web UI:

1. Select **Devices > Device Management**.

The Device Management inventory page displays information about the devices managed in Junos Space Network Management Platform.

2. Select **Device Access > Launch Device WebUI** from the Actions menu.
3. Click the **https://ipaddress** link.

Log in and perform the desired operations, following the instructions for your device.

**Related
Documentation**

- [Viewing Managed Devices on page 41](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Managing Configuration Files Overview on page 444](#)
- [Selecting the Device and the Configuration Perspective on page 54](#)

Changing Device Credentials

You can change the login credentials for any device that Junos Space Network Management Platform manages. Changing the credentials for a managed device updates the credentials in Junos Space Network Management Platform but not on the device itself. To change credentials on a device, you must access the device directly from the CLI.

We recommend that you bring down the managed device connection before you change the login credentials.

To change the login credentials for devices that Junos Space Network Management Platform manages:

1. Select **Devices > Device Management**.

The Device Management inventory page displays information about the devices managed in Junos Space Network Management Platform.



NOTE: You can select one or more devices and apply the same login credentials to the selected devices.

2. Change credentials for one or more managed devices for which the connection status is down as follows:

- a. Select the device or devices for which you want to change login credentials.
- b. Select **Change Credentials** from the Actions menu.
- c. Enter a username and password, and reenter the password.
- d. Click **Confirm**.

The new login credentials for the selected devices are updated in the Junos Space Network Management Platform database.

Change credentials for one or more managed devices for which the connection status is up.

- a. Select one or more devices for which you want to change the login credentials.
- b. Select **Change Credentials** from the Actions menu.

The Change Credentials dialog box appears.

- c. Clear the **Do not change device credentials in the database for devices currently connected to Junos Space** check box.

The Change Credentials dialog box displays the selected devices that are connected to Junos Space Network Management Platform.

- d. Enter a username and password, and reenter the password.
- e. Click **Confirm**.

The new login credentials for the selected devices are updated in the Junos Space Network Management Platform database.

Related Documentation • [Connecting to a Device From Secure Console on page 106](#)

Key-based Authentication Overview

Junos Space Network Management Platform can discover and manage a device either by presenting credentials (username and password) or by key-based authentication.

Junos Space Network Management Platform supports RSA keys for key-based authentication. RSA is an asymmetric-key or public-key algorithm using two keys that are mathematically related. Junos Space Network Management Platform includes a default set of public-private key pairs. However, we recommend that you generate your own public/private key pair with a passphrase applied. Generate your keys by following the instructions in [“Generating and Uploading Authentication Keys to Devices” on page 112](#). The public key can be uploaded to devices being managed by Junos Space Network Management Platform. The private key is encrypted and stored on the system running Junos Space Network Management Platform. Junos Space Network Management

Platform uses username and password credentials to log in to a device for the first time in order to copy and upload the public key. Any further communication to the devices is done using key-based authentication, without passwords.

It is advisable to protect the private key on the Junos Space system by using a passphrase, which is merely a long password that can include spaces and tabs and is much more difficult to break by brute-force guessing than is one shorter string.

You do not have to use RSA-based authentication on every device in your network; you can use passwords on some systems if you prefer or they require it.

Setting up key-based authentication between two computers is a multi-step process that is well described on many IT-related Internet sites (as is the public-key cryptography to which it is related). Junos Space Network Management Platform automates all of this key-creation and uploading process for you. It also tracks and reports the authentication status of each device in the Devices workspace.

**Related
Documentation**

- [Generating and Uploading Authentication Keys to Devices on page 112](#)

Generating and Uploading Authentication Keys to Devices

- [Generating Keys on page 112](#)
- [Uploading Keys to Devices for the First Time on page 113](#)
- [Upload Keys on Managed Devices that have Conflicting keys with Junos Space on page 114](#)
- [Verifying Device Key Status on page 115](#)

Generating Keys

To generate a public/private key pair for authentication during login to network devices:

1. Select **Administration > Fabric** and select the Generate Key icon on the Actions menu. The Key Generator dialog box appears.
2. (Optional) In the **Passphrase** box, enter a passphrase to be used to protect the private key, which will remain on the system running Junos Space Network Management Platform and will be used during device logins.
The passphrase must have a minimum of 5 and a maximum of 255 characters. It may include spaces and tabs. A long passphrase with space and tab characters is harder to break by brute-force guessing. Although a passphrase is not required, it is recommended because it will impede an attacker who gains control of your system and tries to log in to managed network devices.
3. (Optional) Schedule the Junos Space Network Management Platform to generate the keys at a later time.
 - To specify a later start date and time for the key generation, select the **Schedule at a later time** check box.
 - To initiate the key generation as soon as you click **Generate**, clear the **Schedule at a later time** check box (the default).



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

4. Perform one of the following:
 - To generate the keys, click **Generate**.
 - To exit the Key Generator dialog box, click **Cancel**. The keys are not generated.

Uploading Keys to Devices for the First Time

To upload authentication keys to multiple managed devices for the first time:

1. Select **Devices > Device Management**.
The Device Management inventory page appears.
2. On the menu bar, click the **Upload Keys to Devices** icon.
The Upload Keys to Devices dialog box appears.
3. To upload keys to a single device:
 - a. Select **Add Manually**.
The Authentication Details box appears within the Upload Keys to Devices dialog box.
 - b. Select **IP Address** or **Hostname**.
 - c. In the **IP Address/Host Name** box, enter the IP address or the hostname of the target managed device.
 - d. In the **Device Admin** box, enter the appropriate username for that device.
 - e. In the **Password** box, enter the password for that device.
 - f. (Optional) To authorize a different user on the target device, select the **Authorize different user on device** check box and enter the username in the **User on Device** field.

If the username you specify in the **User on Device** field does not exist on the device, a user with this username is created and the key is uploaded for this user. If the **User on Device** field is not specified, then the key is uploaded for the “admin” user on the device.
 - g. Click **Next**.
 - h. Click **Finish** to upload keys to the device.
The Job Information dialog box appears.
 - i. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device. The Job Management page appears. View the job details to know whether this job is successful.
4. To upload keys to multiple devices:

- a. Select **Import From CSV**.
- b. (Optional) To see a sample CSV file as a pattern for setting up your own, select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

You should enter the device name, IP address, device password, and a username on the device. If the username you specify in the user on device column does not exist on the device, a user with this username is created and the key is uploaded for this user. If the user on device column is not specified, then the key is uploaded for "user admin" user on the device.

- c. Once you have a CSV file listing the managed devices and their data, select **Select a CSV To Upload**. The Select CSV File dialog box appears.
- d. Click **Browse** to navigate to where the CSV file is located on the local file system. Make sure that you select a file that has .csv extension.
- e. Click **Upload** to upload keys to the device.

Junos Space Network Management Platform displays the following error if you try to upload non-csv file formats:

Please select a valid CSV file with '.csv' extension.

- f. Click **OK** on the information dialog box that appears. This dialog box displays information about the total number of records that were uploaded and whether this operation was a success.

You can see a green tick mark adjacent to the **Select a CSV To Upload** field, which indicates that the file has been successfully uploaded.

- g. Click **Next**.
- h. Click **Finish**.

The Job Information dialog box appears.

- i. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device. The Job Management page appears. View the job details to know whether this job is successful.

RSA Keys are uploaded automatically to all the managed devices (that were discovered through RSA authentication) in Junos Space, if a new key is generated on Junos Space.

Upload Keys on Managed Devices that have Conflicting keys with Junos Space

To upload authentication keys to one or several managed devices manually:

1. Select **Devices > Device Management**.
The Device Management inventory page appears.
2. Select the check boxes to the left of the names of the devices to which you want to upload keys.
3. On the menu bar, click the **Upload Keys to Devices** icon.

The IP address of the devices are pre-populated.

4. In the **User Name** field, enter the appropriate username for that device.
5. In the **Password** field, enter the password for that device. Confirm it by reentering it in the **Re-enter Password** box.
6. Select **Next** to provide details for the next device.
7. Select **Upload** to upload keys to the managed devices.
The Upload Authentication Key dialog displays a list of the devices with their credentials for your verification.



NOTE: If you do not specify a username in the User Name field, the key is uploaded for “user admin” user on the device. If the username you specify in the User Name field does not exist on the device, a user with this username is created and the key is uploaded for this user.

Verifying Device Key Status

To verify the authentication status of managed devices:

- Select **Devices > Device Management**.
The Device Management inventory page appears.
The Authentication Status column displays one of the following values:
 - **Key Based**—Authentication key was successfully uploaded.
 - **Credentials Based**—Key upload was not attempted; login to this device is by credentials.
 - **Key Conflict**—Junos Space and device do not have the same key.
 - **NA**—“NA” is displayed mostly for LSYS devices and wwJunos devices.

Related Documentation

- [Key-Based Authentication Overview on page 111](#)
- [Device Discovery Overview on page 131](#)
- [Discovering Devices on page 132](#)
- [Resolving Key Conflicts on page 116](#)

Resolving Key Conflicts

Devices connect to Junos Space Network Management Platform using the RSA Key. When the device is disconnected or down, if the a new RSA key is generated from the Administration workspace, the device will not be able to reconnect to Junos Space Network Management Platform when the device comes up. The Authentication Status column in the Device Management page shows that the device is in the Key Conflict state. You can use the Resolve Key Conflict in such instances to resolve the key conflict and provide the new RSA key.

To resolve key conflicts:

1. Select **Devices > Device Management**.
2. Select the devices that are in the Key Conflict state.
3. Right-click and select **Device Access > Resolve Key Conflict** from the contextual menu.
4. Enter the device credentials.

The device is pushed to the Key Based state.

Related Documentation

- [Key-Based Authentication Overview on page 111](#)
- [Changing Device Authentication from Password-based to Key-based Authentication on page 116](#)

Changing Device Authentication from Password-based to Key-based Authentication

Junos Space Network Management Platform supports RSA keys for key-based authentication. Junos Space Network Management Platform automates all of this key-creation and uploading process. It also tracks and reports the authentication status of each device in the Devices workspace. You can also change the authentication mechanism from Password-based to Key-based.

To change the device authentication from password-based to key-based:

1. Select **Devices > Device Management**.
2. Select the devices for which you want to change the authentication from password-based to key-based.
3. Select **Device Access > Modify Authentication** from the contextual menu.

The Modify Authentication window is displayed.

4. Select the **Key Based** option button.
5. Select the devices for which you want to change the authentication from password-based to key-based.
6. In the **Username** field, enter the username of the device.

In case the user does not exist on the device, the user is automatically created.

7. Click **Modify**.

A Job is created. You can view the status of this job in the Job Management workspace.

Related Documentation • [Key-Based Authentication Overview on page 111](#)

CHAPTER 8

Device Monitoring

- [Viewing and Managing Alarms on page 119](#)

Viewing and Managing Alarms

Junos Space Network Management Platform is monitored by default using built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Management Platform > Network Monitoring > Node List), and referred to as Junos Space Network Management Platform node.

There are two basic categories of alarm: acknowledged and outstanding. Acknowledging an alarm indicates that you have taken responsibility for addressing the corresponding network or systems-related issue. Any alarm that has not been acknowledged is considered outstanding and is therefore visible to all users on the Alarms page, which displays outstanding alarms by default.

If an alarm has been acknowledged in error, you can find the alarm and unacknowledge it, making it available for someone else to acknowledge.

When you acknowledge, clear, escalate, or unacknowledge an alarm, this information is displayed in the alarm's detailed view. You can click the alarm ID to view fields such as Acknowledged By, Acknowledgement Type, and Time Acknowledge. These fields display details such as who acknowledged, cleared, escalated, or unacknowledged the alarm; the acknowledgement type (acknowledge, clear, escalate, or unacknowledge); and the date and time the action was performed on the alarm.



NOTE: If a remote user has cleared, acknowledged, escalated, unacknowledged an alarm, the detailed alarm view displays *admin* instead of the actual remote user in the Acknowledged By field.

When you purge alarms, the selected alarms and all corresponding alarm history is purged from the database.

You can search for alarms by entering an individual ID on the initial Alarms page, or by sorting by the column headings on the Alarms page that displays alarms.

- [Viewing Alarms on page 120](#)
- [Acknowledging Alarms on page 122](#)
- [Clearing Alarms on page 122](#)
- [Escalating Alarms on page 122](#)
- [Unacknowledging Alarms on page 122](#)
- [Viewing Acknowledged Alarms on page 123](#)

Viewing Alarms

To view alarms:

1. Select **Network Monitoring > Alarms**.
2. Select one of the following links:
 - All alarms (summary)
 - All alarms (detail)
 - Advanced Search

The Alarms page appears with the list of alarms. By default, the first view for all alarms, both summary and details, shows outstanding alarms, as indicated by the content of the Search constraints box.

3. (Optional) Use the toggle control (the minus sign) in the Search constraints box to show acknowledged alarms.
4. (Optional) You can refine the list of alarms by either or both of the following:
 - Entering information in the Alarm text box.
 - Selecting a time period from the Time list. You can choose only time spans ending now, for example, Last 12 hours.

Select **Search**.

5. (Optional) To view the alarm history for an alarm, select the alarm ID. The alarm history displays the details of previous event or alarm occurrences that map to the event UEI, node ID, IP address, and ifindex of the selected alarm. In addition, when clearing, acknowledging, escalating, or unacknowledging alarms, the alarm action details are also displayed for the corresponding alarms.

The Alarm history provides the following details:

- Event ID
- Alarm ID
- Creation Time
- Severity
- Operation Time

- User
- Operation

Links at the top of the page, under the title, provide access to further functions:

- View all alarms
- Advanced Search
- Long Listing/Short Listing

Table 24 on page 121 describes the information displayed in the columns of the Alarms page. An X indicates that the data is present in the Short Listing or Long Listing displays.

Table 24: Information Displayed in the Alarms List

Data	Short Listing	Long Listing	Comments
Ack check box	X	X	
ID	X	X	Click the ID to go to the Alarm alarm ID section of the Alarms page.
Severity	Color-coding only	X	Toggle enables you to show only alarms with this severity, or not to show alarms with this severity.
UEI		X	Toggle enables you to show only events with this UEI, or not to show events with this UEI.
Node	X	X	Toggles enable you to show only alarms on this IP address, or not to show alarms for this interface.
Interface		X	
Service		X	
Count	X	X	Click the count to view the Events page for the event that triggered this alarm.
Last Event Time	X	X	Mouse over this to see the event ID. Toggles enable you to show only alarms occurring after this event, or only alarms occurring before this event.
First Event Time		X	
Log Msg	X	X	

- Severity Legend—Click to display a table in a separate window showing the full explanations and color coding for the degrees of severity.
- Acknowledge/Unacknowledge entire search—Click to perform the relevant action on all alarms in the current search, including those not shown on your screen.

Acknowledging Alarms

To acknowledge an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Acknowledge Alarms** from the list on the left, and click **Go**.

The alarm is removed from the default view of all users.

Clearing Alarms

To clear an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Clear Alarms** from the list on the left, and click **Go**.

Escalating Alarms

To escalate an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Escalate Alarms** from the list on the left, and click **Go**.

The alarm is escalated by one level.

3. (Optional) To view the severity to which an alarm has been escalated, click the alarm's ID.

Unacknowledging Alarms

To unacknowledge an alarm:

1. Display the list of acknowledged alarms by toggling the Search constraint box so that it shows Alarm is acknowledged.
2. Select the **Ack** check box of the alarm you acknowledged in error. To select all alarms, at the bottom of the page, click **Select All**.
3. At the bottom of the page, select **Unacknowledge Alarms** from the list on the left, and click **Go**.

The alarm appears again in the default view of All Alarms.

Viewing Acknowledged Alarms

To view acknowledged alarms:

1. Select **Network Monitoring > Alarms** and click **All Alarms (summary)** or **All Alarms (details)**.

The Alarms page appears listing the alarms.

2. In the Search constraints field, click the minus sign to toggle between acknowledged and outstanding alarms.
3. (Optional) To remedy an alarm acknowledged by mistake, unacknowledge it.

Related Documentation

- [Viewing, Configuring, and Searching for Notifications on page 395](#)

CHAPTER 9

Custom Attributes

- [Adding Custom Labels on page 125](#)
- [Managing Custom Labels on page 128](#)

Adding Custom Labels

You add custom labels to associate additional data to devices, device interfaces, and device inventory. After you add the custom labels, you can specify the value for these custom labels. Junos Space Network Management Platform provides two pre-defined custom labels - Manufacturer ID and Manufacturer Name. The custom labels and the values are stored in the Junos Space Network Management Platform database. You can view, modify, and delete these custom labels.

The maximum allowed length of the custom Label and value is 255 characters. You cannot add any special characters except spaces and underscore (_) in the name of the label.

- [Adding Custom Labels for a Device on page 125](#)
- [Adding Custom Labels for Physical Inventory on page 126](#)
- [Adding Custom Labels for a Physical Interface on page 127](#)
- [Adding Custom Labels for a Logical Interface on page 127](#)

Adding Custom Labels for a Device

To add custom labels for a device:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management table is displayed.

2. Right-click the device for which you want to add the custom label and select **Manage Customized Attributes**.

The **Manage Customized Attributes** page is displayed.

3. Click the Add label icon.

The Label Name and Value field is displayed. You can either choose a pre-defined label or add a new custom label.

4. To choose a pre-defined label:

- a. Select the pre-defined label from the Label Name dropdown.
 - b. In the **Value** field, enter an appropriate value.
5. To add a new custom label:
 - a. In the **Label Name** dropdown, enter the name for the new label.
 - b. In the **Value** field, enter the value for the new label.
6. Click **Submit**.
7. Click **Close**.

Adding Custom Labels for Physical Inventory

To add custom labels for physical inventory:

1. Select **Network Management Platform > Devices > Device Management**.
The Device Management table is displayed.
2. Right-click the device for which you want to add the custom label and select **Device Inventory > View Physical Inventory** from the contextual menu.
The **View Physical Inventory** page is displayed.
3. Right-click the physical inventory element of the device for which you want to add the custom label and select **Manage Customized Attributes**.
The **Manage Customized Attributes** page is displayed.
4. Click the Add label icon.
The Label Name and Value field is displayed. You can either choose a pre-defined label or add a new custom label.
5. To choose a pre-defined label:
 - a. Select the pre-defined label from the Label Name dropdown.
 - b. In the **Value** field, enter an appropriate value.
6. To add a new custom label:
 - a. In the **Label Name** dropdown, enter the name for the new label.
 - b. In the **Value** field, enter the value for the new label.
7. Click **Submit**.
8. Click **Close**.

Adding Custom Labels for a Physical Interface

To add custom labels for a physical interface:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management table is displayed.

2. Right-click the device for which you want to add the custom label and select **Device Inventory > View Physical Interfaces**.

The **View Physical Interfaces** page is displayed.

3. Right-click the physical interface of the device for which you want to add the custom label and select **Manage Customized Attributes**.

The **Manage Customized Attributes** page is displayed.

4. Click the Add label icon.

The Label Name and Value field is displayed. You can either choose a pre-defined label or add a new custom label.

5. To choose a pre-defined label:

- a. Select the pre-defined label from the Label Name dropdown.
- b. In the **Value** field, enter an appropriate value.

6. To add a new custom label:

- a. In the **Label Name** dropdown, enter the name for the new label.
- b. In the **Value** field, enter the value for the new label.

7. Click **Submit**.

8. Click **Close**.

Adding Custom Labels for a Logical Interface

To add custom labels for a logical interface:

1. Select **Network Management Platform > Devices > Device Management**.

The Device Management table is displayed.

2. Right-click the device for which you want to add the custom label and select **Device Inventory > View Logical Interfaces**.

The **View Logical Interfaces** page is displayed.

3. Right-click the logical interface of the device for which you want to add the custom label and select **Manage Customized Attributes** from the contextual menu.

The **Manage Customized Attributes** page is displayed.

4. Click the Add label icon.

The Label Name and Value field is displayed.

5. In the **Label Name** dropdown, enter the name for the new label.
6. In the **Value** field, enter the value for the new label.
7. Click **Submit**.
8. Click **Close**.

**Related
Documentation**

- [Device Management Overview on page 35](#)
- [Managing Custom Labels on page 128](#)

Managing Custom Labels

You add custom labels to associate additional data to devices, device interfaces, and device inventory. You can modify or delete the custom labels associated with the devices, device interfaces, and device inventory.

- [Modifying Custom Labels on page 128](#)
- [Deleting Custom Labels on page 128](#)

Modifying Custom Labels

To modify a custom label:

1. Select **Network Management Platform > Devices > Device Management**.
The Device Management table is displayed.
2. Right-click the device for which you want to modify the custom label and select **Modify Customized Attributes** from the contextual menu.
3. If you want to modify the custom label associated with a physical interface, logical interface, or the device inventory, navigate to the appropriate page.
4. Select the custom label you want to modify and change the value or the name of the label.
5. Click **Submit**.
6. Click **Close**.

Deleting Custom Labels

To delete a custom label:

1. Select **Network Management Platform > Devices > Device Management**.
The Device Management table is displayed.
2. Right-click the device for which you want to delete the custom label and select **Modify Customized Attributes** from the contextual menu.
3. If you want to delete the custom label associated with a physical interface, logical interface, or the device inventory, navigate to the appropriate page.

4. Select the custom label you want to delete and click the Delete label icon.
5. Click **Submit**.
6. Click **Close**.

Related Documentation

- [Adding Custom Labels on page 125](#)

CHAPTER 10

Discover Devices

- [Device Discovery Overview on page 131](#)
- [Discovering Devices on page 132](#)

Device Discovery Overview

You use device discovery to add devices to Junos Space Network Management Platform. *Discovery* is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space Network Management Platform database. To use device discovery, Junos Space Network Management Platform must be able to connect to the device.

To discover network devices, Junos Space Network Management Platform uses the SSH and SNMP protocols. Device authentication initially is handled through administrator login SSH v2 credentials and SNMP v1/v2c or v3 settings, which are part of the device discovery configuration. You can continue to use credentials for these devices thereafter, or you can create and upload RSA keys to devices to allow Junos Space Network Management Platform to authenticate itself to them automatically during later discoveries.

You can specify a single IP address, a DNS hostname, an IP range, or an IP subnet to discover devices on a network. During discovery, Junos Space Network Management Platform connects to the physical device and retrieves the running configuration and the status information of the device. To connect with and configure devices, Junos Space Network Management Platform uses Juniper Network's Device Management Interface (DMI), which is an extension to the NETCONF network configuration protocol.

When discovery succeeds, Junos Space Network Management Platform creates an object in the Junos Space Network Management Platform database to represent the physical device and maintains a connection between the object and the physical device so their information is linked.

When configuration changes are made in Junos Space Network Management Platform, for example, when you deploy service orders to activate a service on your network devices, the configuration is pushed to the physical device.

If the network is the system of record (NSOR), when configuration changes are made on the physical device (out-of-band CLI commits and change-request updates), Junos Space Network Management Platform automatically resynchronizes with the device so

that the device inventory information in the Junos Space Network Management Platform database matches the current device inventory and configuration information. If Junos Space Network Management Platform is the system of record (SSOR), this resynchronization does not occur and the database is unchanged.

The following device inventory and configuration data is captured and stored in relational tables in the Junos Space Network Management Platform database:

- Devices—hostname, IP address, credentials
 - Physical Inventory—chassis, FPM board, Power Entry Module (PEM), Routing Engine, Control Board (CB), Flexible PIC Concentrator (FPC), CPU, Physical Interface Card (PIC), transceiver (Xcvr), fan tray
- Junos Space Network Management Platform displays the model number, part number, serial number, and description for each inventory component, when applicable.
- Logical Inventory—subinterfaces, encapsulation (link-level), type, speed, maximum transmission unit (MTU), VLAN ID
 - License information:
 - License usage summary—license feature name, feature description, licensed count, used count, given count, needed count
 - Licensed feature information—original time allowed, time remaining
 - License SKU information—start date, end date, and time remaining
 - Loopback interface

Other device configuration data is stored in the Junos Space Network Management Platform database as binary large objects, and is available only to northbound interface (NBI) users.

Related Documentation

- [Discovering Devices on page 132](#)
- [Viewing Managed Devices on page 41](#)
- [Systems of Record in Junos Space Overview on page 733](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Device Management Overview on page 35](#)
- [Device Inventory Overview on page 40](#)
- [Managing DMI Schemas Overview on page 714](#)

Discovering Devices

You use device discovery to automatically discover and synchronize Junos OS devices in Junos Space Network Management Platform. Device discovery is a three-step process

in which you specify target devices, a probe method (ping or SNMP or both, or none), and, optionally, credentials to connect to each device.



NOTE: The values that you enter to specify the targets, probe method, and credentials are persistent from one discovery operation to the next, so you do not have to reenter information that is the same from one operation to the next.



NOTE: To perform discovery on a device with dual Routing Engines, always specify the IP address of the current master Routing Engine. When the current master IP address is specified, Junos Space Network Management Platform manages the device and the redundancy. If the master Routing Engine fails, the backup Routing Engine takes over and Junos Space Network Management Platform manages the transition automatically without bringing down the device.



NOTE: When you initiate discovery on a device, Junos Space Network Management Platform automatically enables the NETCONF protocol over SSH by pushing the following command to the device:

```
set system services netconf ssh
```

To discover and synchronize devices, complete the following tasks:

1. [Specifying Device Targets on page 133](#)
2. [Specifying Probes on page 135](#)
3. [Specifying Credentials on page 136](#)

Specifying Device Targets

To specify the device targets that you want Junos Space Network Management Platform to discover:

1. Select **Devices > Device Discovery > Discover Targets**.

The Discover Targets dialog box appears.

2. You can add devices using either the **CSV Upload** button or the Add icon, or both together.

Use the **CSV Upload** feature to add devices in bulk. You can add hundreds of devices to Junos Space Network Management Platform by using a CSV file that contains information extracted from an LDAP repository.

To view a sample CSV file, click the **CSV Sample** link.

- The **File Download** dialog box appears.
- Click **Open** to view a sample CSV file.



NOTE: Steps 4–7 below are optional if you use only the Add icon to add devices. Steps 8–10 below are optional if you use only the CSV Upload button to add devices. Follow steps 4–10 if you use both the CSV Upload button and the Add icon to add devices.

3. Click the **CSV Upload** button to add your own CSV files.



NOTE: The format of the CSV file that you are uploading should exactly match the format of the sample CSV file.

A dialog box appears.

4. Click **Browse**.

The CSV File Upload dialog box appears.

5. Navigate to the desired CSV file, select it, and then click **Open**.

The CSV File Upload dialog box reappears, this time displaying the name of the selected file.

6. Click **Upload** to upload the selected CSV file.

7. Click the Add icon to add devices by specifying IP addresses, IP address range, IP subnet, or host name.

The Add Device Target dialog box appears.

8. Choose one of the following options to specify device targets:

- Select the **IP** option button and enter the IP address of the device.
- Select the **IP Range** option button and enter a range of IP addresses for the devices. The maximum number of IP addresses for an IP range target is 1024.
- Select the **IP subnet** option button and enter an IP subnet for the devices.
- Select the **Host name** option button and enter the hostname of the device.

9. Click **Add** to save the target devices that you specified, or click **Add More** to add more device targets. When you have added all device targets that you want Junos Space Network Management Platform to discover, click **Add**.

The Discover Targets Dialog box displays the addresses of the configured device targets.

10. Click **Discover** from the Discover Targets dialog box.



NOTE: You need to navigate through the Specify Probes and Specify Credentials dialog boxes before you click the Discover button.

In the next task, you specify a probe method to connect to and discover the device targets.

Specifying Probes

To configure the method Junos Space Network Management Platform uses to discover the device targets:

1. Select **Devices > Device Discovery > Specify Probes**.

The Specify Probes dialog box appears.

2. Select a probe method (or SSH) to discover target devices:

- If SNMP is configured for the device, select **Use SNMP**, and clear the check box **Use Ping**.

Junos Space Network Management Platform uses the SNMP GET command to discover target devices.

- If SNMP is not configured for the device, select the check box **Use Ping**, and clear the check box **Use SNMP**.

Junos Space Network Management Platform uses the Juniper Networks Device Management Interface (DMI) to directly connect to and discover devices. DMI is an extension to the NETCONF network management protocol.

- When both the Use Ping and Use SNMP check boxes are selected (the default), Junos Space Network Management Platform can discover the target device more quickly, if the device is pingable and SNMP is enabled on the device.

3. Click the Add icon (+).

An Add SNMP Settings dialog box appears.

4. The following figure shows the Add SNMP Settings dialog box when you select **SNMP V1/V2C**. If you make this selection, specify a community string, which can be **public**, **private**, or a predefined string.

Figure 16: Modify SNMP Setting Dialog Box

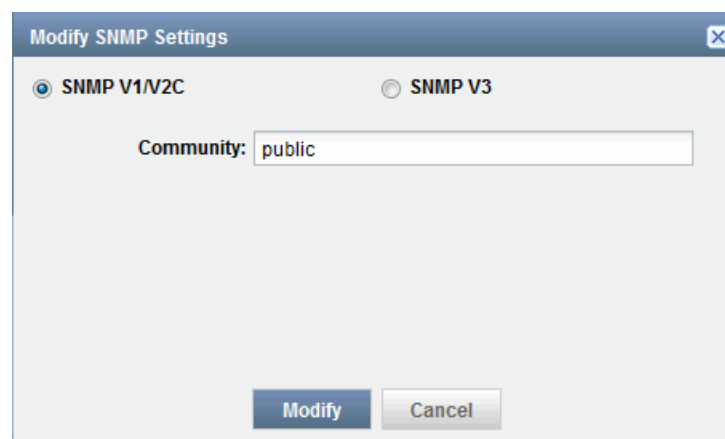


Figure 17 on page 136 shows the Add SNMP Settings dialog box when you select **SNMP V3**.

Figure 17: SNMP v3 Options

If you make this selection, complete the following settings:

- Enter the username.
- Select the privacy type (**AES 128**, **DES**, or **none**).
- Enter the privacy password (if AES 128 or DES). If you specify **none** for the privacy type, the privacy function is disabled.
- Select the authentication type (**MD5**, **SHA**, or **none**).
- Enter the authentication password (if MD5 or SHA). If you specify **none** for the authentication type, the authentication function is disabled.

Click **Add** to save the SNMP settings, or click **Add More** to add additional configurations. After using **Add More**, click **Add** to save the settings and close the dialog box.

The Specify Probes dialog box displays the configured SNMP settings.

5. Click **Discover** in the Specify Probes dialog box.

Specifying Credentials

Optionally, specify an administrator name and password to establish the SSH connection for each target device that you configured. If you are using key-based authentication, you do not need to do this step.

1. Select **Devices > Device Discovery > Specify Credentials**.

The Specify Credentials dialog box appears.

2. Click the Add icon.

The Add Device Login Credential dialog box appears.

3. Specify the administrator username and password, and confirm the password. The name and password must match the name and password configured on the device.

Save the user name and password that you specified by selecting **Add** or **Add More** to add another username and password. If you use Add More, select **Add** after you have finished adding all login credentials.

The Credential dialog box displays the administrator user names that you configured.

4. Schedule the device discovery operation:

- Clear the **Schedule at a later time** check box (the default) to initiate the discovery operation when you complete Step 7 in this procedure.
- Select the **Schedule at a later time** check box to specify a later start date and time for the discovery operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but is mapped to the local time zone of the client computer.

5. Select **Discover** to start the discovery job.

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

6. To view device discovery details, select **View Detailed Report**.

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



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

You can also view the device discovery job in the Jobs workspace.

To view device discovery from the Jobs workspace:

1. Select **Jobs > Job Management**.
The Job Management inventory page appears.
2. Enter **Discover Network Elements** in the search box to view device discovery jobs.

Related Documentation

- [Viewing Managed Devices on page 41](#)
- [Viewing Scheduled Jobs on page 466](#)
- [Resynchronizing Managed Devices With the Network on page 94](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)
- [Viewing Physical Inventory on page 73](#)
- [Viewing Physical Interfaces on page 76](#)
- [Exporting License Inventory on page 80](#)
- [Managing DMI Schemas Overview on page 714](#)
- [Key-Based Authentication Overview on page 111](#)

Deployed Devices

- [Adding Deployed Devices on page 139](#)
- [Add Deployed Devices Wizard Overview on page 141](#)
- [Managing Deployed Devices on page 142](#)
- [Adding SRX Series Devices Overview on page 143](#)
- [Adding Devices on page 145](#)
- [Deploying Device Instances on page 149](#)

Adding Deployed Devices

To create a Task Instance:

1. Select **Devices > Deployed Devices > Add Devices**.
2. In the Name box, enter a name for the new Task Instance.
3. In the Description box, enter a description for the new Task Instance.
4. You can add a new Task Instance either by importing a CSV file or manually.

To add a new Task Instance by importing a CSV file:

- a. Select the **Import to CSV** option button.
- b. Select the **View Sample CSV** link in the Import section to see a sample of the CSV file that should be uploaded.
- c. Save the sample CSV file to your storage location.
- d. Make necessary changes in this CSV file and rename it with an appropriate name.



NOTE: Do not add or delete any columns in the CSV file. You cannot upload the CSV file successfully if you add or delete any columns.

- e. Select the **Select a CSV To Upload** link in the Import section.

The **Select CSV File** dialog box appears.

- f. Click **Browse** and upload the CSV file from your storage location.

- g. If the CSV file is successfully uploaded, a Green mark appears next to the Select a CSV To Upload link.

The Upload dialog box appears.

- h. Click **OK**.

To add a new Task Instance manually:

- a. Select the **Add Manually** option button.
- b. Enter the following details in the Device Details section:
 - From the Platform list, select an appropriate platform.
 - From the OS Version list, select an appropriate OS version.
 - In the Number of devices box, enter the number of devices with the same platform and OS version.





NOTE: If you add multiple devices, a unique numerical identifier is appended at the end of each device name.

- c. In the Authentication Details section:
 - In the Username box, choose an appropriate user name.
 - In the Password box, enter a password.
 - In the Re-enter Password box, reenter the password.

5. Click **Next**.

6. This wizard page displays rows that make up the configured Task Instance. Select a row or rows and use the icons described in [Table 25 on page 140](#) to view or download management CLI commands.

Table 25: Icons to View or Download Management CLI Commands

Icon	Description
	View the management CLI commands.
	Download the management CLI commands.

7. Click **Finish**.

The new Task Instance you have added appears in the Add Deployed Devices inventory page. A new job is created and the job ID appears in the Job Information dialog box.

8. Click the job ID to view more information about the job created.

This action directs you to the Job Management workspace.

- Related Documentation**
- [Add Deployed Devices Wizard Overview on page 141](#)
 - [Managing Deployed Devices on page 142](#)
 - [Managing DMI Schemas Overview on page 714](#)

Add Deployed Devices Wizard Overview

Network devices deployed on the network can be easily managed by Junos Space Network Management Platform using the Discover Devices task. However, for security devices, SSH and ping are disabled on the device interface for any incoming traffic. Hence, security devices cannot communicate with Junos Space Network Management Platform. In such instances, you can use the Add Deployed Devices Wizard to enable communication between security devices and Junos Space Network Management Platform. The Add Deployed Devices Wizard creates a Task Instance that you can use to obtain management CLI commands related to these devices. These CLI commands can be pasted on the device console, enabling the device to connect to Junos Space Network Management Platform for further management.

You can create Task Instances either manually or by uploading a comma-separated values (CSV) file. You need to specify the following details to create a Task Instance:

- Device name
- Device platform
- OS version
- Device count
- Authentication details

You can store the management CLI commands obtained from a Task Instance and paste it on the device console or on a command-line session on the device.



NOTE:

If you are using Internet Explorer to download the management CLI commands, you must customize the browser settings to download them. Perform the following steps to customize the Internet Explorer settings:

1. Open Internet Explorer and select Tools > Internet Options.
 2. Click the Security tab and select the Custom Level tab.
 3. In the Automatic prompting for file downloads section, click the Enable option button.
-

- Related Documentation**
- [Adding Deployed Devices on page 139](#)
 - [Managing Deployed Devices on page 142](#)
 - [Managing DMI Schemas Overview on page 714](#)

Managing Deployed Devices

Task Instances are listed in the Add Deployed Devices inventory page. You can view or download the management CLI commands associated with Task Instances. You can also view the device instance status or delete Task Instances.

This topic describes the following tasks related to Task Instances and management CLI commands:

- [Viewing the Details of a Task Instance on page 142](#)
- [Viewing the Device Status on page 142](#)
- [Deleting a Task Instance on page 143](#)
- [Downloading Management CLI Commands on page 143](#)

Viewing the Details of a Task Instance

To view the details of a Task Instance:

1. From the task tree, select the **Devices** workspace.
Graphical summaries about the devices in the network appear.
2. Expand the **Devices** workspace by clicking the expansion symbol to the left of its name.
Tasks related to managing devices are displayed in the expanded portion of the tree.
3. Select **Deployed Devices**.
The Deployed Devices inventory page appears.
4. Double-click the row for the Task Instance whose details you intend to view.
The details of the Task Instance are displayed in the Add Instance Details dialog box.
5. Click **Close** to close the Add Instance Details dialog box.

Viewing the Device Status

To view the device status:

1. Select **Devices > Deployed Devices**.
The Deployed Devices inventory page appears.
2. Select the Task Instance for which you intend to view the device status, and click **View Device Status** from the Actions menu.
A new dialog box displays the connection status and managed status of the devices.
3. Click **Back** on the top-left corner to return to the inventory page.

Deleting a Task Instance

To delete a Task Instance you have created:

1. Select **Devices > Deployed Devices**.

The Deployed Devices inventory page appears.

2. Select the Task Instance you intend to delete and click the **Delete** link from the Actions menu.

The Delete Instance dialog box appears.

3. Select the Task Instance you want to delete and click **Delete**.

Downloading Management CLI Commands

To download management CLI commands from the Task Instance you have created:

1. From the task tree, select **Devices > Deployed Devices**.

The Deployed Devices inventory page appears.

2. Select the Task Instance containing the management CLI commands you intend to download and click the **Download Management CLIs** link from the Actions menu.

The Download Management CLIs dialog box appears.

3. Click the **Download Management CLIs** link.
4. Save the .zip file in your local host.

Related Documentation

- [Add Deployed Devices Wizard Overview on page 141](#)
- [Adding Deployed Devices on page 139](#)
- [Managing DMI Schemas Overview on page 714](#)

Adding SRX Series Devices Overview

You can use the Add Device wizard to create deployment instances that are used to deploy SRX Series devices. You can create deployment instances either manually or by uploading a comma-separated values (CSV) file. A deployment instance contains the configlets used to deploy branch SRX Series devices that are currently using the factory default settings.

A configlet is a small subset of a configuration used by a device to obtain an IP address and connect back to the management station for further management. A configlet contains information about the device series, device platform, OS version, and the connection details used to bootstrap the device. It can be used to deploy devices from an external storage device such as a USB stick.

You need to specify the following details to create a configlet:

- Device name
- Device series
- Device platform
- OS version
- Device count
- Connectivity type
- Interface
- Connection profile
- Encryption password

You can store this configlet in an external USB storage device and plug it into the SRX Series device to start it. The device count and encryption option determine the subsequent steps in starting the SRX Series device using the configlet.

The following parameters determine the steps in booting the SRX Series device using the configlet:

- Plain text configlet

If you save the configlet as a plain text file, the device will not prompt you to enter a password during the startup process.

- Encrypted configlet using AES encryption with a custom key

If you encrypt the configlet with a custom key, the device will prompt you to enter a password. You are required to enter the 16-character password specified during the creation of the configlet. You can also save a text file named `key.txt` in the USB storage device that you are using to start the device. This file contains the password; the device will automatically use the password specified in this file.

- Device count value is 1

If you create an individual configlet for each device with a Device Count column value of 1, the configlet contains the hostname. The device does not prompt you to enter the hostname during startup.

- Device count value greater than 1

You can start devices with similar network connection parameters (for example, obtaining IP address through DHCP) using an individual configlet. This is done by specifying the number of devices that can be started with the same configlet in the Device Count column. If you create such a configlet, the device prompts for a hostname during startup. You are required to enter a unique hostname for each of the devices that are used to startup using this configlet. You can also save a text file named `hostname.txt` in the USB storage device which you are using to start the device. This file contains the hostnames for all devices that are started using the configlet.



NOTE: By default, the configlet that you download is named Configlets.zip. This zip file is unzipped to obtain the configlet files. You should not rename the configlet files. Renaming the configlet files may not complete the device startup process.



NOTE: If you are using Internet Explorer to download the configlets, you need to customize the browser settings to download them. Perform the following steps:

1. Open Internet Explorer and navigate to Tools > Internet Options.
2. Click the Security tab and select the Custom Level tab.
3. In the Automatic prompting for file downloads section, click the Enable option button.

Related Documentation

- [Adding Devices on page 145](#)
- [Deploying Device Instances on page 149](#)
- [Managing DMI Schemas Overview on page 714](#)

Adding Devices

This topic includes the following procedures:

- [Creating a Deployment Instance on page 145](#)
- [Adding a Deployment Instance by Importing a CSV File on page 146](#)
- [Adding a Deployment Instance Manually on page 147](#)
- [Working with Rows and Columns on page 147](#)
- [Working with Configlets on page 149](#)

Creating a Deployment Instance

To create a new deployment instance:

1. From the task tree, select the **Devices** workspace.
Graphical summaries about the devices in the network appear.
2. Expand the **Devices** workspace by clicking the expansion symbol to the left of its name.
Tasks related to managing devices are displayed in the expanded portion of the tree.
3. Expand the **Add Deployed Devices** workspace by clicking the expansion symbol to the left of its name.
The Add Deployed Devices inventory page appears.
4. From the task tree, select **Add Devices**.

The Add Devices dialog box appears.

5. In the Name box, enter a name for the new deployment instance.
6. In the Description box, enter a description for the new deployment instance.
7. Add a new deployment instance either by importing or manually adding a CSV file. See [“Adding a Deployment Instance by Importing a CSV File” on page 146](#) or [“Adding a Deployment Instance Manually” on page 147](#).
8. Click **Next**.

The Add Devices dialog box appears, displaying a table of settings for the deployment instance that you have added manually or uploaded using a CSV file. Each record in the table can be used to create a configlet.

9. Implement the configlet. See [“Working with Rows and Columns” on page 147](#) and [“Working with Configlets” on page 149](#).
10. Click **Finish**.

The new deployment instance you have added appears in the Device Details inventory page. A new job is created and the job ID appears in the Job Information dialog box.

11. Click the job ID to view more information about the job created.

This action directs you to the Job Management workspace.



NOTE: When you have a large number of devices, we recommend you wait for the Job to complete before downloading the configlets.

Adding a Deployment Instance by Importing a CSV File

To add a new deployment instance by importing a CSV file:

1. Select the **Import to CSV** option button.
2. Select the **View Sample CSV** link in the Import section to view a sample of a CSV file.
3. Save the sample CSV file to your storage location.
4. Make necessary changes in this CSV file and rename it with an appropriate name.



NOTE: Do not add or delete any columns in the CSV file. You cannot upload the CSV file successfully if you add or delete any columns.

5. Select the **Select a CSV To Upload** link in the Import section.
6. The Select CSV File dialog box appears.
7. Click **Browse** and upload the CSV file from your storage location.

If the CSV file is successfully uploaded, a Green mark appears next to the Select a CSV To Upload link.

The Upload dialog box appears.

8. Click **OK**.

Adding a Deployment Instance Manually

To add a new deployment instance manually:

1. Select the **Add Manually** option button.
2. Enter the following details in the Device Details section:
 - From the Platform list, select an appropriate platform.
 - From the OS Version list, select an appropriate OS version.
 - In the Number of devices box, enter the number of devices with the same connection details.

These devices will use a common connection profile.

3. Enter the following details in the Connectivity Details section:
 - Specify an Interface Type: Ethernet or ADSL.
 - The Interface box displays the default interface in the untrust zone, depending on the connection type chosen. Make changes to this field if necessary.
 - Select an appropriate IP assignment type.
 - Select an appropriate connection profile.

Working with Rows and Columns

The Rapid Deployment dialog box displays a table of settings for the deployment instance that you have added manually or uploaded using a CSV file. Each record in the table can be used to create a configlet.

You can clone, delete, sort the rows, and hide the columns in the Rapid Deployment dialog box.

[Table 26 on page 148](#) describes the icons used to perform these tasks.

Table 26: Icons in the Rapid Deployment dialog box





Icon	Description
	<p>View the details of a configlet.</p> <p>To view a configlet:</p> <ol style="list-style-type: none"> 1. Select the check box to the left of the row corresponding to the configlet you want to view. 2. Click the View Configlet icon.
	<p>Clone a row from the deployment instance table.</p> <p>To clone rows:</p> <ol style="list-style-type: none"> 1. Select the check boxes to the left of the rows you want to clone. 2. Specify the number of clones in the Clone Times field. 3. Click the Clone icon. <p>The new rows appear at the end of the table.</p>
	<p>Delete a row from the deployment instance table.</p> <p>To delete rows:</p> <ol style="list-style-type: none"> 1. Select check boxes to the left of the rows you want to delete. 2. Click the Delete icon
	<p>Download configlets.</p> <p>To download the configlets:</p> <ol style="list-style-type: none"> 1. Select the check boxes to the left of the rows corresponding to the configlets you want to download. 2. Click the Download Configlet icon. <p>NOTE: If you are using Internet Explorer to download the configlets, you need to customize the browser settings to be able to download them. Perform the following steps to customize the Internet Explorer settings:</p> <ol style="list-style-type: none"> 1. Open Internet Explorer and navigate to Tools > Internet Options. 2. Click the Security tab and select the Custom Level tab. 3. In the Automatic prompting for file downloads section, click the Enable option button.

Table 27 on page 148 lists the fields that you need to add manually.

Table 27: Fields Manually Entered in the Rapid Deployment Dialog Box

Field	Description
Device Count	Specify the number of devices that can be deployed using this configlet.
Interface IP	Specify the IP address of the interface.

Table 27: Fields Manually Entered in the Rapid Deployment Dialog Box (*continued*)

Field	Description
Gateway	Specify the IP address of the gateway.

Working with Configlets

You can use the procedures in this section to package the configlet.

To encrypt the configlet:

1. Select the type of encryption you want to use in the Encryption section: AES or Plain Text.
2. Enter a password with 16 characters in the corresponding field.



NOTE: You will need to provide this password when you deploy devices using this configlet.

To save the configlet to a disk drive:

- Click the **Click Here** link next to the field in the Save section.

To save the configlet to an FTP location:

1. Select the option button corresponding to the file transfer method you want to use.
2. Enter the user ID, password, server address and folder details in the appropriate fields.

Related Documentation

- [Adding SRX Series Devices Overview on page 143](#)
- [Deploying Device Instances on page 149](#)
- [Managing DMI Schemas Overview on page 714](#)

Deploying Device Instances

You can view, delete and search for specific deployment instances listed in the Deploy Devices inventory page. You can also download configlets from a specific deployment instance.

You can perform the following tasks on the deployment instances and configlets:

1. [Viewing the Details of a Deployment Instance on page 150](#)
2. [Viewing the Device Status on page 150](#)
3. [Deleting a Deployment Instance on page 150](#)
4. [Downloading Configlets on page 150](#)
5. [Searching for a Deployment Instance on page 151](#)

Viewing the Details of a Deployment Instance

To view the details of a deployment instance:

1. From the task tree, select **Devices > Deployed Devices**.

The Deploy Devices inventory page appears.

2. Double-click the icon for the deployment instance whose details you intend to view.

The Deployment Instance Details report appears.

3. Click **Close**.

Viewing the Device Status

To view the device status:

1. From the task tree, select **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. Select the deployment instance you intend to view the device status for and click the **View Device Status** link from the Actions menu in the left corner of the inventory page.

A dialog box displays the connection status of the devices.

3. Click **Back** on the left corner of this dialog box to return to the inventory page.

Deleting a Deployment Instance

To delete a deployment instance you have created:

1. From the task tree, select the **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. Select the deployment instance you intend to delete and click the **Delete** link from the Actions menu in the left corner of the inventory page.

The Delete Deployment Instance dialog box appears.

3. Select the deployment instance you want to delete and click **Delete**.

Downloading Configlets

To download the configlet you have created:

1. From the task tree, select **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. Select the deployment instance containing the configlet you intend to download and click the **Download Configlets** link from the Actions menu in the left corner of the inventory page.

The Download Configlets dialog box appears.

3. Select the **Download XML based Configlets** link in the Download Configlets dialog box.
4. Save the .zip file in your storage location.



NOTE: You can also download the configlets when you are creating a deployment instance. However, for a large number of devices we recommended downloading the configlets from the inventory page. See [“Adding Devices” on page 145](#).



NOTE: You cannot download the configlets associated with a deployment instance if a job related to that deployment instance is in progress. The Download Configlets action is disabled until the job is completed.

Searching for a Deployment Instance

To search for a deployment instance you have created:

1. From the task tree, select **Devices > Deploy Devices**.
The Deploy Devices inventory page appears.
2. In the Search box, enter the name of the deployment instance you want to search.
3. Click the magnifying glass icon next to the Search box.

The Deploy Devices inventory page is populated with the deployment instances matching your search criterion.

Related Documentation

- [Adding SRX Series Devices Overview on page 143](#)
- [Adding Devices on page 145](#)

Unmanaged Devices

- [Adding Unmanaged Devices on page 153](#)

Adding Unmanaged Devices

In the Junos Space Network Management Platform context, unmanaged devices are those made by vendors other than Juniper Networks, Inc. You can add such devices to Junos Space Network Management Platform manually, or by importing multiple devices simultaneously from a CSV file. You need to provide the IP address or the host name of the non-Juniper devices. The other details such as the vendor names, SNMP credentials, and the loopback address details. If Junos Space Network Management Platform can communicate with the device using SNMP, the information gathered via SNMP overrides the information that you enter.

Creating an unmanaged device from a vendor other than Juniper Networks also creates a tag for that vendor (for example, CISCO) and assigns that tag to the device.

To add a non-Juniper device to Junos Space Network Management Platform manually:

1. Select **Network Management Platform - Devices > Unmanaged Devices**.
The Add Unmanaged Devices page appears.
2. Select the **Add Manually** option button.
The Device Details area appears.
3. Select **Host Name** or **IP Address**.
The first box changes to represent your selection. Enter the appropriate name or address value for the device.
4. (Optional) In the **Vendor** box, enter the name of the device's vendor.
The maximum length is 256 characters. Spaces are acceptable.
5. Select the **Configure Loopback** check box if you want to configure the loopback address for the device. If you do so, the Loopback Settings area appears. This is an optional field.
 - a. In the **Loopback Name** field, enter the loopback name for the device.
 - b. In the **Loopback Address** field, enter the loopback address for the device.

The loopback address should be a valid IP address in the range of 1.0.0.0 to 223.255.255.255

6. Select the **SNMP** box if you want to use SNMP to gather device information. If you do so, the SNMP Settings area appears.
7. Use the option buttons to select either SNMP V1/V2C or SNMP V3.
 - If you select SNMP V1/V2C, the Community box appears. Enter the appropriate SNMP community string (password) to give access to the device.
 - If you select SNMP V3, several boxes appear, as described in [Table 28 on page 154](#). Enter values as appropriate.

Table 28: SNMP V3 Configuration Parameters

Name	Value
Username	The username previously configured on the device.
Authentication type	The algorithm used for authentication: MD5, SHA1, or None. MD5 or SHA1 is used to create a hash of the authentication password. Note that only this password is encrypted, not any other packets transmitted.
Authentication password	The password that authenticates Junos Space Network Management Platform to the device to gain access to it. The password must have at least eight characters and can include alphanumeric and special characters, but not control characters.
Privacy type	The encryption algorithm: AES128, DES, or None, used to encrypt transmitted packets.
Privacy password	The password that allows reading the transmissions themselves. The password must have at least eight characters.

8. Press **Finish** to complete the addition of this device.

To add a non-Juniper device or multiple devices to Junos Space Network Management Platform using a CSV file:

1. Select **Devices > Add Unmanaged Devices**.
The Add Unmanaged Devices page appears.
2. Select the **Import from CSV** option button.
The **Import** area appears, displaying the following links:
 - View Sample CSV
 - Select a CSV file to Upload.

Clicking **View Sample CSV** displays a CSV file with the format shown in [Table 29 on page 154](#).

Table 29: Sample CSV for Importing Unmanaged Devices

Column Heading	Sample Data	Field Constraints
Host Name or IP Address	Sunnyvale_R1	Name: Limit of 256 characters, no spaces. IP address: Dotted decimal notation.

Table 29: Sample CSV for Importing Unmanaged Devices (*continued*)

Column Heading	Sample Data	Field Constraints
Vendor	ABC	Alphabetic characters only
Device UserName	root	No validation from Junos Space Platform
Device Password	root123	No validation from Junos Space Platform
SNMP Version	SNMPV3	SNMPv3, or SNMPv1 or v2C
Community	N/A (for SNMP V3)	Community string (authentication password) for V2; otherwise, N/A
SNMP Username	admin	Username for SNMP V3; otherwise N/A
Authentication Type	MD5	MD5, SHA1, or N/A
Authentication Password	admin123	Must have at least eight characters and can include alphanumeric and special characters, but not control characters
Privacy Type	DES	DES, AES128, or N/A
Privacy Password	admin123	Must have at least eight characters and can include alphanumeric and special characters, but not control characters. Can be same as authentication password, or different.
Loopback Name	lo0	The loopback name for the device.
Loopback Address	127.0.0.1	The loopback address for the device. The loopback address should be a valid IP address in the range of 1.0.0.0 to 223.255.255.255

3. Once you have a complete CSV file, select **Select a CSV file to Upload**.

4. Click **Next**.

The Add Managed Devices page displays the list of unmanaged devices with their details.

5. Click **Finish**.

You are redirected to the Unmanaged Devices page.



NOTE: You should enter a valid loopback address or enter “N/A” in the Loopback Address column. If you enter an invalid loopback address or leave the cell empty, the associated unmanaged device is not added to Junos Space Network Management Platform.

Related Documentation • [Device Management Overview on page 35](#)

- [Viewing Managed Devices on page 41](#)

Secure Console

- [Configuring SRX Device Clusters in Junos Space on page 157](#)

Configuring SRX Device Clusters in Junos Space

You can create a cluster of two SRX-series devices that are combined to act as a single system, or create a single-device cluster and then add a second device to the cluster later. You can also configure a standalone device from an existing cluster device.



NOTE: You can discover and manage SRX device clusters in Junos Space Network Management Platform.

This topic includes the following tasks:

- [Configuring a Standalone Device from a Single-node Cluster on page 157](#)
- [Configuring a Standalone Device from a Two-Node Cluster on page 159](#)
- [Configuring a Primary Peer in a Cluster from a Standalone Device on page 160](#)
- [Configuring a Secondary Peer in a Cluster from a Standalone Device on page 161](#)

Configuring a Standalone Device from a Single-node Cluster

You can configure a standalone device from device that is currently configured as a single-node cluster.

To configure a single-node cluster as a standalone device:

1. Select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the single-node cluster device.



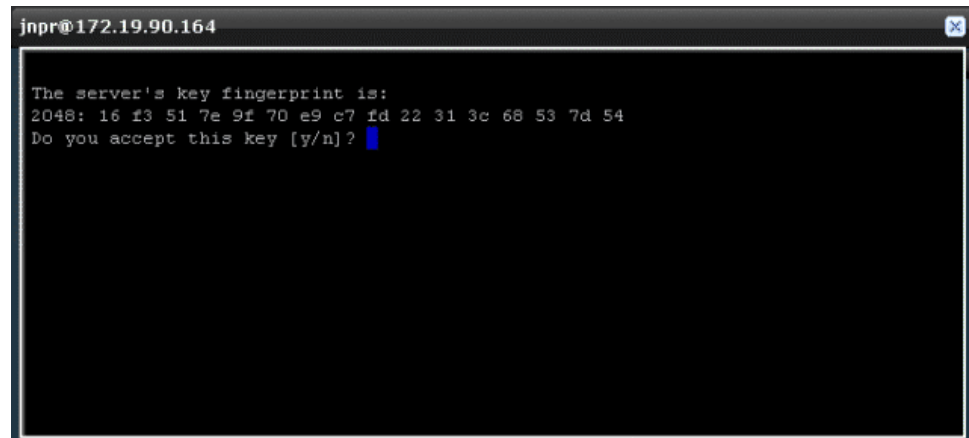
NOTE: A device in a single-node cluster is always the primary member.

3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.

4. Click **Connect**.

The device key fingerprint window appears, as shown in the following example.

Figure 18: Validating the Server Key Fingerprint



5. Verify that the fingerprint is for the device you want to connect to, then type **y** and press Enter to validate the Server's key fingerprint.

A terminal window opens in a non-modal popup with an SSH connection opened on the selected device.

6. Enter the set chassis command to remove the cluster configuration:

```
set chassis cluster cluster-id 0 node 0
```

7. Reboot the device, by entering the command:

```
request system reboot
```

8. Copy the outbound-ssh configuration from group node to system level, for example:

```
set system services outbound-ssh client 00089BBC494A device-id 6CFF68
set system services outbound-ssh client 00089BBC494A secret "$ABC123"
set system services outbound-ssh client 00089BBC494A services netconf
set system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804
```

9. Copy the system log configuration from group node to system level:

```
set system syslog file default-log-messages any any
set system syslog file default-log-messages structured-data
```

10. Copy the fxp0 interface setting from group node to system level, for example:

```
set interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

11. Delete the outbound-ssh configuration from the group node, for example:

```
delete groups node0 system services outbound-ssh
```

12. Delete the system log configuration from the group node, for example:

```
delete groups node0 system syslog file default-log-messages any any
delete groups node0 system syslog file default-log-messages structured-data
```

13. Delete the interfaces configuration from the group node, for example:

```
delete groups node0 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

14. Commit the configuration changes on the device:

```
commit
```

In the Junos Space user interface, the device connection status will go down and then up again. After the device connection is back up, you can verify that the device you configured displays as a standalone device.

15. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
16. Click in the top right corner of the terminal window to close the window.

Configuring a Standalone Device from a Two-Node Cluster

You can configure a standalone device from the secondary peer device in a cluster.



NOTE: You cannot use the primary peer in a two-node cluster to configure a standalone device.

To configure a secondary peer device in a cluster as a standalone device:

1. Select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the secondary peer device.
3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.
4. Click **Connect**.

The device key fingerprint window appears, as shown in the following example.

5. Verify that the fingerprint is for the device you want to connect to, then type **y** and press Enter to validate the Server's key fingerprint.

A terminal window opens in a non-modal popup with an SSH connection opened on the selected device.

6. Disconnect the HA cable from the device that you want to configure as a standalone device.
7. Enter the set chassis command for the peer device, for example:

```
set chassis cluster cluster-id 0 node 1
```

8. Reboot the device, by entering the command:

```
request system reboot
```

9. Copy the outbound-ssh configuration from group level to system level, for example:

```
set system services outbound-ssh client 00089BBC494A device-id 6CFF68
set system services outbound-ssh client 00089BBC494A secret "SABC123"
set system services outbound-ssh client 00089BBC494A services netconf
set system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804
```

10. Copy the system log configuration from group level to system level:

```
set system syslog file default-log-messages any any
set system syslog file default-log-messages structured-data
```

11. Copy the fxp0 interface setting from group level to system level, for example:

```
set interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

12. Delete the outbound-ssh configuration from the group level, for example:

```
delete groups node1 system services outbound-ssh
```

13. Delete the system log configuration from the group level, for example:

```
delete groups node1 system syslog file default-log-messages any any
delete groups node1 system syslog file default-log-messages structured-data
```

14. Delete the interfaces configuration from the group level, for example:

```
delete groups node1 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

15. Commit the configuration changes on the device:

```
commit
```

In the Junos Space user interface, the device connection status will go down and then up again. After the device connection is back up, you can verify that the device you configured displays as a standalone device.

After the device connections are up, verify the following changes in the Manage Devices inventory landing page:

- The device you configured now displays as a standalone device.
- The cluster that formerly included a primary and secondary peer device now displays the primary peer device only.

16. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
17. Click in the top right corner of the terminal window to close the window.

Configuring a Primary Peer in a Cluster from a Standalone Device

You can create a device cluster from two standalone devices. Use the following procedure to configure a standalone device as the primary peer in a cluster.

To configure a primary peer in a cluster from a standalone device:

1. Select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the standalone device that you want to configure as the primary peer in the cluster.

3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.

4. Click **Connect**.

The device key fingerprint window appears.

5. Verify that the fingerprint is for the device you want to connect to, and type **y** and press Enter to validate the Server's key fingerprint.

A terminal window opens in a non-modal popup with an SSH connection opened on the selected device.

6. For the standalone device, enter the command:

```
set chassis cluster cluster-id 1 node 0
```

7. Reboot the device, by entering the command:

```
request system reboot
```

8. Copy the outbound-ssh configuration from the system level to the group level, for example:

```
set groups node0 system services outbound-ssh client 00089BBC494A device-id 6CFF68  
set groups node0 system services outbound-ssh client 00089BBC494A secret "$ABC123"  
set groups node0 system services outbound-ssh client 00089BBC494A services netconf  
set groups node0 system services outbound-ssh client 00089BBC494A 10.155.70.252 port  
7804
```

9. Copy the fxp0 interface configuration from the system level to the group level, for example:

```
set groups node0 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

10. Copy the system log configuration from system level to group level:

```
set groups node0 system syslog file default-log-messages any any  
set groups node0 system syslog file default-log-messages structured-data
```

11. Delete the outbound-ssh configuration from the system level, for example:

```
delete system services outbound-ssh
```

12. Delete the system log configuration from the system level, for example:

```
delete system syslog file default-log-messages any any  
delete system syslog file default-log-messages structured-data
```

13. Delete the interfaces configuration from the system level, for example:

```
delete interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

14. Commit the configuration changes on the device again:

```
commit
```

After the device connection is up, verify the following changes:

- In the Manage Devices inventory landing page:
 - The cluster icon appears for the device.
 - The new cluster device appears as the primary device.
 - In the physical inventory landing page, Junos Space Network Management Platform displays chassis information for the primary device cluster.
15. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
 16. Click in the top right corner of the terminal window to close the window.

Configuring a Secondary Peer in a Cluster from a Standalone Device

If a device cluster contains only a primary peer, you can configure a standalone device to function as a secondary peer in the cluster. Use the following procedure to ensure that Junos Space Network Management Platform is able to manage both devices.

To add a standalone device to a cluster:

1. Select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the standalone device that you want to configure as a secondary peer in a cluster.
3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.

4. Click **Connect**.

The device key fingerprint window appears.

5. Verify that the fingerprint is for the device you want to connect to, and type **y** and press Enter to validate the Server's key fingerprint.

A terminal window opens in a non-modal popup with an SSH connection opened on the selected device.

From the terminal window prompt, you can enter CLI commands to create a standalone device from the device cluster.

6. For the standalone device, enter the command:

```
set chassis cluster cluster-id 1 node 1
```

7. Enter the command:

```
request system reboot
```

8. Copy the outbound-ssh configuration from the system level to the group level, for example:

```
set groups node1 system services outbound-ssh client 00089BBC494A device-id 6CFF68
set groups node1 system services outbound-ssh client 00089BBC494A secret "$ABC123"
set groups node1 system services outbound-ssh client 00089BBC494A services netconf
set groups node1 system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804
```

9. Copy the fxp0 interface configuration from the system level to the group level, for example:

```
set groups node1 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

10. Copy the system log configuration from system level to group level:

```
set groups node1 system syslog file default-log-messages any any
set groups node1 system syslog file default-log-messages structured-data
```

11. Delete the outbound-ssh configuration from the system level, for example:

```
delete system services outbound-ssh
```

12. Delete the system log configuration from the system level, for example:

```
delete system syslog file default-log-messages any any
delete system syslog file default-log-messages structured-data
```

13. Delete the interfaces configuration from the system level, for example:

```
delete interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

14. Commit the configuration changes on the device again:

```
commit
```

15. Connect the HA cable to each device in the cluster.
16. Establish an SSH connection to the primary device in the cluster.
17. On the primary device, make some trivial change to the device, for example, add a description, and commit the change:
commit
After the device connections are up for both devices in the cluster, verify the following changes:
 - In the Manage Devices inventory landing page:
 - Each peer device displays the other cluster member.
 - The cluster icon appears for each member device.
 - One device appears as the primary device and the other as the secondary device in the cluster.
 - In the physical inventory landing page, chassis information appears for each peer device in the cluster.
18. To terminate the SSH sessions, type **exit** from the terminal window prompt, and press Enter.
19. Click in the top right corner of the terminal window to close the window.

CHAPTER 14

Manage Device Adapter

- [Worldwide Junos OS Adapter Overview on page 165](#)
- [Installing the Worldwide Junos OS Adapter on page 166](#)

Worldwide Junos OS Adapter Overview

The Junos Space wwadapter enables you to manage devices running the worldwide version of Junos OS (ww Junos OS devices) through Junos Space Network Management Platform.

ww Junos OS devices use Telnet instead of Secure Shell (SSH2) to communicate with other network elements. Junos Space Network Management Platform uses the failover approach when identifying a ww Junos OS device. It first tries to initiate a connection to the device using SSH2. If it cannot connect to the device, Junos Space Network Management Platform identifies the device as a ww Junos OS device. Since Junos Space Network Management Platform does not support Telnet, it uses an adapter to communicate with ww Junos OS devices. Junos Space Network Management Platform connects to the adapter using SSH2 and the adapter starts a Telnet session with the device.

Before you install the wwadapter, complete the following prerequisites:

- Download the adapter image from the local client workstation.
- Ensure that the Junos Space servers have been deployed and are able to access devices.
- Configure Junos Space Network Management Platform to initiate connections with the device.



NOTE: Ensure that you allow at least three Telnet connections between the ww Junos OS device and the Junos Space server. Junos Space Network Management Platform needs a minimum of three Telnet connections with the device in order to be able to manage it.



NOTE: For ww Junos OS devices, the Junos Space Service Now application works only on AI-Scripts version 2.5R1 and later.

The Secure Console workspace and the option in the right-click context menu in the Manage Devices workspace are disabled for ww Junos OS devices.

For more information, see [“Installing the Worldwide Junos OS Adapter” on page 166](#).

Related Documentation

- [Installing the Worldwide Junos OS Adapter on page 166](#)

Installing the Worldwide Junos OS Adapter

This section shows you how to install and use the wwadapter to manage devices running on the worldwide version of Junos OS (ww Junos OS devices).

This section includes the following tasks:

- [Installing the wwadapter Image on page 166](#)
- [Connecting to ww Junos OS Devices on page 167](#)

Installing the wwadapter Image

Before you install the wwadapter, you must upload the ww Junos OS device wwadapter image file.

To upload the wwadapter image file:

1. Select **Devices > Device Adapter**.
2. Select the Add Device Adapter icon on the menu bar.
3. Browse to the wwadapter image file and select the filename so that the full path appears in the Software File field.
4. Click **Upload** to bring the image into Junos Space Network Management Platform.

A status box shows the progress of the image upload. Adding the wwadapter image file automatically installs the wwadapter.

Before you connect to any device, you must verify that the installation was successful.

To verify that the installation was successful, look at the device console on the Space server.

1. On the server, change directories to verify that the wwadapter directory has been created.

```
cd /home/jmp/wwadapter
```

2. To verify that the wwadapter is running, enter the following command on the Space server:

```
prompt > service wwadapter status
```

wwadapter running

If the wwadapter is not active, you see the following status:

wwadapter stopped

Use the following commands to start or stop the wwadapter:

To start the wwadapter:

service wwadapter start

To stop the wwadapter:

```
prompt > ps -ef | grep wwadapter
prompt > kill -9 {wwadapter pid}
```

To see the wwAdapter logs, change directories to the wwadapter directory.

```
cd /home/jmp/wwadapter/var/errorLog/DmiAdapter.log
```

To view the contents of the error log file, open it with any standard text editor.

To view the contents of the log4j configuration file, change directories to the wwadapter directory.

```
cd /home/jmp/wwadapter /wwadapterlog4j.lcf
```

Connecting to ww Junos OS Devices

A device running worldwide Junos OS (ww Junos OS device) cannot initiate a connection with Junos Space Network Management Platform. Junos Space Network Management Platform must initiate the connection to the device. To configure this setting:

1. Select **Administration > Applications**.

The Applications page appears displaying all the applications currently running in the Junos Space server.

2. Select **Network Management Platform** and select **Modify Application Settings** from the Actions dropdown.

The Modify Application Settings page appears.

3. Select **Junos Space initiates connection to device**.
4. Select **Support ww Junos Devices** so that Junos Space Network Management Platform can connect to a ww Junos OS device using the wwadapter.

After Junos Space Network Management Platform has discovered the ww Junos OS device through the wwadapter ([“Discovering Devices” on page 132](#)), it manages the device just as it would manage a device that runs the domestic version of Junos OS.



NOTE: The Secure Console workspace and the SSH to Device option on the right-click contextual menu in the Manage Devices workspace are disabled for ww Junos OS devices.



NOTE: If you are not able to discover the WW Junos OS device , make sure that the NMAP utility returns ‘telnet’ as open for port 23 on the device.

```
$ nmap -p23 < Device IP >
```

**Related
Documentation**

- [Modifying Junos Space Application Settings on page 624](#)

CHAPTER 15

Upload Keys to Devices

- [Key-based Authentication Overview on page 169](#)
- [Generating and Uploading Authentication Keys to Devices on page 170](#)

Key-based Authentication Overview

Junos Space Network Management Platform can discover and manage a device either by presenting credentials (username and password) or by key-based authentication.

Junos Space Network Management Platform supports RSA keys for key-based authentication. RSA is an asymmetric-key or public-key algorithm using two keys that are mathematically related. Junos Space Network Management Platform includes a default set of public-private key pairs. However, we recommend that you generate your own public/private key pair with a passphrase applied. Generate your keys by following the instructions in [“Generating and Uploading Authentication Keys to Devices” on page 112](#). The public key can be uploaded to devices being managed by Junos Space Network Management Platform. The private key is encrypted and stored on the system running Junos Space Network Management Platform. Junos Space Network Management Platform uses username and password credentials to log in to a device for the first time in order to copy and upload the public key. Any further communication to the devices is done using key-based authentication, without passwords.

It is advisable to protect the private key on the Junos Space system by using a passphrase, which is merely a long password that can include spaces and tabs and is much more difficult to break by brute-force guessing than is one shorter string.

You do not have to use RSA-based authentication on every device in your network; you can use passwords on some systems if you prefer or they require it.

Setting up key-based authentication between two computers is a multi-step process that is well described on many IT-related Internet sites (as is the public-key cryptography to which it is related). Junos Space Network Management Platform automates all of this key-creation and uploading process for you. It also tracks and reports the authentication status of each device in the Devices workspace.

Related Documentation

- [Generating and Uploading Authentication Keys to Devices on page 112](#)

Generating and Uploading Authentication Keys to Devices

- [Generating Keys on page 170](#)
- [Uploading Keys to Devices for the First Time on page 170](#)
- [Upload Keys on Managed Devices that have Conflicting keys with Junos Space on page 172](#)
- [Verifying Device Key Status on page 173](#)

Generating Keys

To generate a public/private key pair for authentication during login to network devices:

1. Select **Administration > Fabric** and select the Generate Key icon on the Actions menu. The Key Generator dialog box appears.
2. (Optional) In the **Passphrase** box, enter a passphrase to be used to protect the private key, which will remain on the system running Junos Space Network Management Platform and will be used during device logins.
The passphrase must have a minimum of 5 and a maximum of 255 characters. It may include spaces and tabs. A long passphrase with space and tab characters is harder to break by brute-force guessing. Although a passphrase is not required, it is recommended because it will impede an attacker who gains control of your system and tries to log in to managed network devices.
3. (Optional) Schedule the Junos Space Network Management Platform to generate the keys at a later time.
 - To specify a later start date and time for the key generation, select the **Schedule at a later time** check box.
 - To initiate the key generation as soon as you click **Generate**, clear the **Schedule at a later time** check box (the default).



.....

NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

.....

4. Perform one of the following:
 - To generate the keys, click **Generate**.
 - To exit the Key Generator dialog box, click **Cancel**. The keys are not generated.

Uploading Keys to Devices for the First Time

To upload authentication keys to multiple managed devices for the first time:

1. Select **Devices > Device Management**.
The Device Management inventory page appears.
2. On the menu bar, click the **Upload Keys to Devices** icon.

The Upload Keys to Devices dialog box appears.

3. To upload keys to a single device:

a. Select **Add Manually**.

The Authentication Details box appears within the Upload Keys to Devices dialog box.

b. Select **IP Address** or **Hostname**.

c. In the **IP Address/Host Name** box, enter the IP address or the hostname of the target managed device.

d. In the **Device Admin** box, enter the appropriate username for that device.

e. In the **Password** box, enter the password for that device.

f. (Optional) To authorize a different user on the target device, select the **Authorize different user on device** check box and enter the username in the **User on Device** field.

If the username you specify in the **User on Device** field does not exist on the device, a user with this username is created and the key is uploaded for this user. If the **User on Device** field is not specified, then the key is uploaded for the "admin" user on the device.

g. Click **Next**.

h. Click **Finish** to upload keys to the device.

The Job Information dialog box appears.

i. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device. The Job Management page appears. View the job details to know whether this job is successful.

4. To upload keys to multiple devices:

a. Select **Import From CSV**.

b. (Optional) To see a sample CSV file as a pattern for setting up your own, select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

You should enter the device name, IP address, device password, and a username on the device. If the username you specify in the user on device column does not exist on the device, a user with this username is created and the key is uploaded for this user. If the user on device column is not specified, then the key is uploaded for "user admin" user on the device.

c. Once you have a CSV file listing the managed devices and their data, select **Select a CSV To Upload**. The Select CSV File dialog box appears.

d. Click **Browse** to navigate to where the CSV file is located on the local file system. Make sure that you select a file that has .csv extension.

e. Click **Upload** to upload keys to the device.

Junos Space Network Management Platform displays the following error if you try to upload non-csv file formats:

Please select a valid CSV file with '.csv' extension.

- f. Click **OK** on the information dialog box that appears. This dialog box displays information about the total number of records that were uploaded and whether this operation was a success.

You can see a green tick mark adjacent to the **Select a CSV To Upload** field, which indicates that the file has been successfully uploaded.

- g. Click **Next**.

- h. Click **Finish**.

The Job Information dialog box appears.

- i. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device. The Job Management page appears. View the job details to know whether this job is successful.

RSA Keys are uploaded automatically to all the managed devices (that were discovered through RSA authentication) in Junos Space, if a new key is generated on Junos Space.

Upload Keys on Managed Devices that have Conflicting keys with Junos Space

To upload authentication keys to one or several managed devices manually:

1. Select **Devices > Device Management**.
The Device Management inventory page appears.
2. Select the check boxes to the left of the names of the devices to which you want to upload keys.
3. On the menu bar, click the **Upload Keys to Devices** icon.
The IP address of the devices are pre-populated.
4. In the **User Name** field, enter the appropriate username for that device.
5. In the **Password** field, enter the password for that device. Confirm it by reentering it in the **Re-enter Password** box.
6. Select **Next** to provide details for the next device.
7. Select **Upload** to upload keys to the managed devices.
The Upload Authentication Key dialog displays a list of the devices with their credentials for your verification.



NOTE: If you do not specify a username in the User Name field, the key is uploaded for “user admin” user on the device. If the username you specify in the User Name field does not exist on the device, a user with this username is created and the key is uploaded for this user.

Verifying Device Key Status

To verify the authentication status of managed devices:

- Select **Devices > Device Management**.

The Device Management inventory page appears.

The Authentication Status column displays one of the following values:

- **Key Based**—Authentication key was successfully uploaded.
- **Credentials Based**—Key upload was not attempted; login to this device is by credentials.
- **Key Conflict**—Junos Space and device do not have the same key.
- **NA**—"NA" is displayed mostly for LSYS devices and wwJunos devices.

Related Documentation

- [Key-Based Authentication Overview on page 111](#)
- [Device Discovery Overview on page 131](#)
- [Discovering Devices on page 132](#)
- [Resolving Key Conflicts on page 116](#)

PART 3

Device Templates

- [Overview on page 177](#)
- [Template Definitions on page 183](#)
- [Templates on page 209](#)

CHAPTER 16

Overview

- [Device Templates Overview on page 177](#)

Device Templates Overview

- [Device Templates Overview on page 178](#)
- [Device Templates Workflow on page 181](#)
- [Viewing Statistics for Templates and Definitions on page 181](#)
- [User Privileges in Device Templates on page 182](#)
- [Changing Template Definition States on page 182](#)

Device Templates Overview

The Device Templates workspace provides the tools to create custom device templates deployable through Junos Space Network Management Platform. Unlike other systems that provide configuration of most aspects of a device and allow implementation of some form of template, Device Templates enables you to set *all* configuration parameters for *any* supported device because it is DMI schema-driven. In other words, all Juniper devices managed by Junos Space Network Management Platform convey to the system all their parameters, which are displayed for configuration in the Configuration Editor and in Device Templates.

Templates are an excellent way to create the base build of a new device. Using device templates, you can configure, for example, routing protocols such as bgp, ospf, isis or even static routes. You can even set up CSV files (outside of Junos Space Network Management Platform) as a basis for your template definitions.



NOTE: When you deploy a template to a device, even the unconfigured parameters are committed. This means that if you applied two templates to a device, only the configuration contained in the last template would be retained. For example, if you set SNMP location in the first template you deployed, but did not do so in the second template, the SNMP location information would be lost as soon as you deployed the second template. Therefore, to build up a complex configuration by applying multiple templates in stages, you should modify the last deployed definition or template each time you add a layer of complexity.

This behavior also has implications for versioning. In order for Space to retain version information, every time a template is deployed to a device, the previous template deployed to the device is undeployed, even if the subsequent template only contains additional parameter settings. In other words, template deployment is not additive.

The device templates workflow has two [predefined] roles:

- The Template Design Manager—A designer who understands both:
 - The technical details of device configuration
 - How to implement this knowledge to solve specific business problems
- The Template Manager—An operator, a junior individual to execute the orders of the designer.

A template design manager (hereinafter referred to as a “designer”) creates template definitions and publishes them. A template manager (hereinafter referred to as an operator”) selects a template definition and creates from it a template to configure one or more devices. The operator then tests the template on the device (without deploying it). If the template is validated, the operator deploys the template to the devices.

With this division of labor, the operator does not need specialist knowledge. The designer can design the device templates to allow (or prevent) specific tasks to be performed by specified administrator roles. Alternatively, one person can have both roles.

While creating the definition, the designer can verify what the operator sees when creating a template from the definition. The operator, however, can gain no insight into what the designer saw when creating the definition. This has important consequences: while the designer can identify configuration options simply through their place in the hierarchy represented as a tree, the operator is entirely dependent on the name of the option. It is by means of the label alone that an operator determines which parameter he or she is configuring.

Designers can choose not only which options to display to their operators, but also whether to display them at all. They can make configuration options editable or read-only, and even provide customized explanations for operators.

Operators can immediately deploy a template to the devices they select, or schedule deployment for a later date. With Junos Space Network Management Platform as the System of Record (in the SSOR mode), the operator can deploy a template on a device in two ways:

- Assign a template to a device by using the **Assign to Device** workflow in the Device Templates workspace, and approve and deploy the template by using the **Review/Deploy Configuration** workflow in the Devices workspace.
- Deploy a template to a device using the **Deploy** workflow in the Device Templates workspace.

If you assign a template to a device and use the Deploy workflow to deploy that template on the same device, the template is not deployed to the device. The managed status of the device is shown as "Space Changed" in the Device Management page.



NOTE: You cannot edit, publish, or delete a template definition if the template definition is being edited by another user. You will receive a pop-up message indicating the user who is currently editing the template definition.



NOTE: You cannot edit or delete a template if the template is being edited by another user. You will receive a pop-up message indicating the user who is currently editing the template.



NOTE: We recommend that you do not navigate to other pages or other Junos Space applications when modifying a template or a template definition. Save the changes before you navigate to other pages or other Junos Space applications.

**Related
Documentation**

- [Device Templates Workflow on page 181](#)

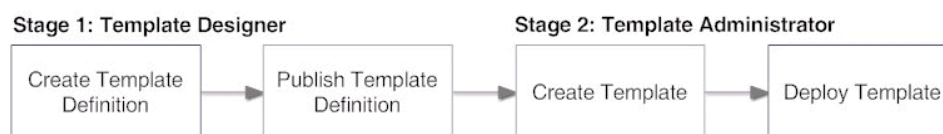
Device Templates Workflow

The device templates workflow has two parts, corresponding to the two roles associated with this workspace:

- The Template Design Manager, or template designer, who creates the template definition (see [“Creating a Template Definition Overview” on page 188](#)).
- The Template Manager, or template administrator, who creates a template from a template definition (see [“Creating a Template Overview” on page 222](#)).

Figure 19 on page 181 diagrams the role responsibilities and the workflow for creating a definition, then a template from the definition, and finally deploying the template to devices.

Figure 19: Workflow for Device Template Definition and Template Creation



Related Documentation

- [Creating a Template Definition Overview on page 188](#)
- [Creating a Template Overview on page 222](#)

Viewing Statistics for Templates and Definitions

The device template statistics page shows the states of both definitions and templates, and the number of templates per device family.

All the charts are interactive. Clicking the enabled templates part of the Template Status chart, for example, takes you directly to the page displaying that category of template.



NOTE: Do not use your browser's Back and Forward buttons to navigate in Device Templates pages.

The Device Templates statistics page displays the following information:

- **Template Status**—this pie chart shows the templates that are enabled, disabled, and needing review. The templates based on a definition that is currently in a published state are enabled. Templates based on a definition that is currently unpublished are disabled. Templates based on a republished definition are marked as needing review.
- **Template Definition Status**—this pie chart shows published and unpublished definitions (available for template creation and unavailable, respectively).
- **Template Count by Device Family**—this bar chart shows the number of templates per device family (each template can apply to only one device family).

- Related Documentation**
- [Changing Template Definition States on page 182](#)
 - [Viewing Template Inventory on page 225](#)
 - [Viewing Template Definition Inventory on page 185](#)
 - [Managing Template Definitions on page 183](#)
 - [Publishing and Unpublishing a Template Definition on page 184](#)

User Privileges in Device Templates

In Junos Space Network Management Platform Users, the two roles for Device Templates users are predefined: Template Design Manager for the definition designer and Template Manager for the operator. For ease of use, in this documentation we refer to the Template Design Manager as the designer, and to the Template Manager as the operator.

You must have Template Design Manager privileges to create, delete, modify, and manage template definitions.

You must have Template Manager Privileges to create, deploy, delete, modify, and manage templates.

- Related Documentation**
- [Role-Based Access Control Overview on page 479](#)

Changing Template Definition States

When a designer finishes creating a template definition, that definition is automatically published by default. Designers can perform a series of operations on definitions, but to do so, they must first unpublish the definitions. Operators can see only published definitions; unpublished ones are not visible for them.

Ensure that you have the appropriate permissions before undertaking any of these tasks or operations. See [“User Privileges in Device Templates” on page 182](#)

- To be available for use by operators, template definitions must be published. Template definitions that are unpublished are not available for the creation of templates.
- Templates based on a definition that was unpublished after the templates were created are automatically disabled.
- Templates based on a definition that was unpublished and then republished are marked as needing review. They cannot be deployed before the operator reviews them.
- Templates based on a definition that has been deleted are permanently disabled.
- Templates based on a published definition that has not been unpublished in the meantime are enabled.

- Related Documentation**
- [Publishing and Unpublishing a Template Definition on page 184](#)
 - [Creating a Template Definition Overview on page 188](#)
 - [Creating a Template on page 223](#)

CHAPTER 17

Template Definitions

- [Manage Definitions on page 183](#)
- [Create Definition on page 188](#)
- [Manage CSV Files on page 204](#)
- [Import Definitions on page 205](#)

Manage Definitions

- [Managing Template Definitions on page 183](#)
- [Publishing and Unpublishing a Template Definition on page 184](#)
- [Modifying a Template Definition on page 185](#)
- [Viewing Template Definition Inventory on page 185](#)
- [Cloning a Template Definition on page 186](#)
- [Deleting a Template Definition on page 187](#)
- [Exporting a Template Definition on page 187](#)

Managing Template Definitions

Before you begin, make sure you have the appropriate permissions; see [“User Privileges in Device Templates” on page 182](#).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in Device Templates pages.

To manage Device Template definitions, from the task tree, navigate to the Definitions inventory page by selecting **Device Templates > Definitions**. The Definitions inventory page displays all published or unpublished template definitions in a table format view. You can select or deselect all items, and you can use the search function to find a template definition by name.

From the Definitions page, you can use the Actions menu to publish, unpublish, modify, view, clone, delete, import, and export a template definition. You can also tag and untag an object.

- Related Documentation**
- [Creating a Template Definition Overview on page 188](#)
 - [Publishing and Unpublishing a Template Definition on page 184](#)
 - [Modifying a Template Definition on page 185](#)
 - [Deleting a Template Definition on page 187](#)
 - [Importing a Template Definition on page 206](#)
 - [Exporting a Template Definition on page 187](#)
 - [Cloning a Template Definition on page 186](#)
 - [Managing Templates Overview on page 209](#)
 - [Changing Template Definition States on page 182](#)

Publishing and Unpublishing a Template Definition

In the lifecycle of a definition there are two states.



NOTE: If you unpublish a definition that is already being used as the basis for templates, all templates based on that definition are disabled. Republishing the definition alone is not enough to reenable the templates. The templates must be reviewed before they can be reenabled (see [“Managing Templates Overview” on page 209](#)).

1. To view all template definition states, select **Device Templates > Definitions**.



TIP: To use an existing published definition as the basis for a new definition, clone the existing definition and make your modifications to the clone (see [“Cloning a Template Definition” on page 186](#)).

To publish a template definition:

1. Select **Device Templates > Definitions**, and select the definition.
2. Select **Publish Template Definition** or **Unpublish Template Definition** or select the appropriate command from the Actions menu.

If you try to unpublish a definition already being used for templates, the **Unpublish Template Definition** dialog box notifies you that in unpublishing, you will disable those templates, and prompts you to confirm you want to do this.

- Related Documentation**
- [Cloning a Template Definition on page 186](#)
 - [Modifying a Template Definition on page 185](#)
 - [Changing Template Definition States on page 182](#)

Modifying a Template Definition

You can modify a template definition only when it is unpublished.

To modify a published definition, you must first unpublish it (see [“Publishing and Unpublishing a Template Definition” on page 184](#)).

When you modify a template definition, you cannot change the device family. Also, by default, the same OS and schema versions are used as in the original template definition.

When you modify a template definition, you cannot change any existing pages. You can only add additional pages.

To modify a template definition:

1. Select **Device Templates > Definitions** and select the definition by clicking its check box.
2. Select **Modify Template Definition** or select the appropriate command from the Actions menu.
3. To make the modified definition available to operators, publish it.



NOTE: Because you must unpublish a definition before modifying it, any templates based on that definition are disabled. After you modify a definition and republish, templates based on that definition are not automatically reenabled. The status of the affected templates is **Needs Review**.

Related Documentation

- [Publishing and Unpublishing a Template Definition on page 184](#)
- [Cloning a Template Definition on page 186](#)
- [Deleting a Template Definition on page 187](#)
- [Importing a Template Definition on page 206](#)
- [Exporting a Template Definition on page 187](#)

Viewing Template Definition Inventory

To view Device Template definition inventory, select **Device Templates > Definitions**. The Definitions inventory page appears.

You can display template definitions in tabular view. You can also do the following:

- Use the Search function to find a particular template definition.
- Select all template definitions on a page, or you can deselect them.
- You can refresh the page by clicking the Refresh icon in the status bar.
- When you have selected a template definition, you can perform actions on it by right-clicking it or hovering over the Actions menu.

- Related Documentation**
- [Managing Template Definitions on page 183](#)
 - [Publishing and Unpublishing a Template Definition on page 184](#)
 - [Modifying a Template Definition on page 185](#)
 - [Cloning a Template Definition on page 186](#)
 - [Deleting a Template Definition on page 187](#)
 - [Importing Template Definitions Overview on page 205](#)
 - [Importing a Template Definition on page 206](#)
 - [Exporting a Template Definition on page 187](#)

Cloning a Template Definition

Cloning a template definition is the same as copying it. If you want to copy a definition from one Junos Space fabric to another, however, you must import or export it.

To modify a template definition without disabling templates based upon that definition, first clone the definition, then modify the clone.

Unlike the **Modify** function, the **Clone** function does not require that a definition be unpublished.

When you clone a template definition, you cannot change the device family or any existing pages.

To add additional pages, modify the clone (see [“Modifying a Template Definition” on page 185](#)).

To clone a template definition:

1. Select **Device Templates > Definitions**, and select the definition by clicking its check box.
2. Select **Clone Template Definition** from the Actions menu.

The new definition appears, named **Clone of ...**

3. To make the cloned definition available to operators, publish it (see [“Publishing and Unpublishing a Template Definition” on page 184](#)).

- Related Documentation**
- [Deleting a Template Definition on page 187](#)
 - [Modifying a Template Definition on page 185](#)
 - [Publishing and Unpublishing a Template Definition on page 184](#)
 - [Importing Template Definitions Overview on page 205](#)

Deleting a Template Definition

You can delete a template definition only when it is unpublished. This status is indicated by an appropriate icon. A different icon indicates a published definition.

To delete a published definition, you must first unpublish it (see [“Publishing and Unpublishing a Template Definition” on page 184](#)). When you unpublish a definition, any templates based on that definition are disabled. When you delete a definition, all templates based on that definition are permanently disabled. They can therefore be neither modified nor deployed.

To delete a template definition:

1. Select **Device Templates > Definitions**, and select the definition.
2. Select **Delete** from the Actions menu.



TIP: Ensure that you have a plan in place before you delete a definition that is being used for templates. All templates based on a deleted definition are disabled.

Related Documentation

- [Publishing and Unpublishing a Template Definition on page 184](#)
- [Cloning a Template Definition on page 186](#)
- [Modifying a Template Definition on page 185](#)
- [Changing Template Definition States on page 182](#)

Exporting a Template Definition

Exporting a template definition enables you to transfer it to another Junos Space fabric.

Before you begin, you must have a template definition already created.

To export a definition:

1. From the Definitions page, select the definition to export.
2. Select **Export** from the Actions menu.

The Export Template Definition dialog box appears.

3. Click **Download file for selected template definitions (tgz format)**.

The Opening xxx.tgz dialog box appears. (XXX is a placeholder for the name of the definition.)

4. Select **Save File** and click **OK**.

You may have to toggle between the option buttons to activate the **OK** button.

The Enter name of file to save to ... dialog appears.

5. Rename the file if desired and save it to the appropriate location.

The Export Template Definition dialog reappears.

6. Click **Close**.

Although the exported definition file is an .XML file, it is saved as a .tgz file, which is the format the system uses to import XML files.

You can now import the definition into another Junos Space fabric.

Related Documentation

- [Importing Template Definitions Overview on page 205](#)
- [Importing a Template Definition on page 206](#)
- [Cloning a Template Definition on page 186](#)
- [Managing Template Definitions on page 183](#)

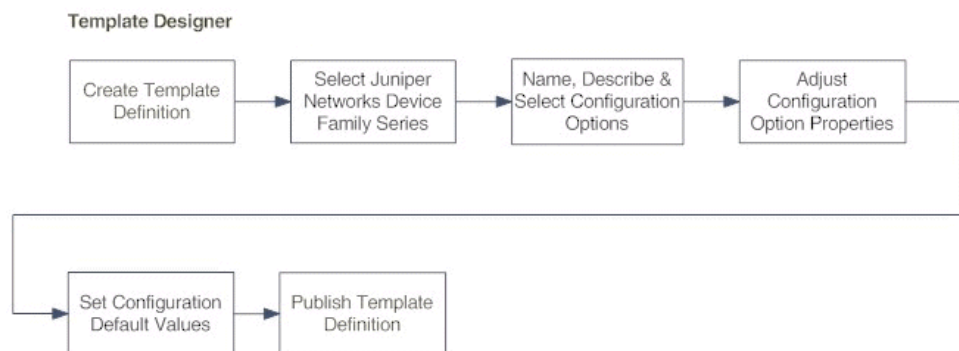
Create Definition

- [Creating a Template Definition Overview on page 188](#)
- [Creating a Template Definition on page 189](#)
- [Finding Configuration Options on page 199](#)
- [Specifying Device-Specific Values in Definitions on page 200](#)
- [Working with Rules on page 203](#)

Creating a Template Definition Overview

The workflow for creating a template definition is illustrated by [Figure 20 on page 188](#).

Figure 20: Template Definition Workflow



Creating a template definition includes the following tasks, described in “[Creating a Template Definition](#)” on page 189, unless specified otherwise:

1. Select a device family.
2. Select the configuration options (parameters) to be included in the definition. .

3. Define the text, labels, and template UI elements the operator sees, which includes defining which options or parameters the operator sees and can change in the template.
4. Determine which - if any - parameters will be governed by CSV files or rules. See [“Specifying Device-Specific Values in Definitions” on page 200](#), [“Managing CSV Files” on page 204](#), and [“Working with Rules” on page 203](#).
5. Set the default values for the template parameters, i.e. the range of permissible values the operator can enter.
6. Preview the template and if necessary modify the definition. See [“Modifying a Template Definition” on page 185](#).



NOTE: Template definitions are published by default. If you want to avoid making a definition available to operators, you must unpublish it. See [“Publishing and Unpublishing a Template Definition” on page 184](#).

Related Documentation

- [Device Templates Overview on page 178](#)
- [Device Templates Workflow on page 181](#)

Creating a Template Definition

- [Selecting the Device Family and Naming the Definition on page 189](#)
- [Creating Configuration Pages on page 190](#)
- [Determining Editable Parameters on page 192](#)
- [Filling in the General Tab on page 193](#)
- [Filling in the Description Tab on page 195](#)
- [Filling in the Validation Tab on page 196](#)
- [Filling in the Advanced Tab on page 197](#)
- [Specifying Default Values for Configuration Options on page 198](#)

Selecting the Device Family and Naming the Definition

Each template definition is associated with a Juniper Networks Device Family DMI schema. Before creating any template definitions, you must set a default DMI schema for each device family. See [“Setting a Default DMI Schema” on page 722](#).

To select the device family and name the template definition:

1. Select **Device Templates**.

The Device Templates statistics page appears, displaying all available statistics for both template definitions and templates.

2. Select **Definitions**.

The Templates inventory page appears, displaying all template definitions.

3. Click the **Create Template Definition** icon on the menu bar.

The Create Template Definition page appears.

4. From the Device Family Series panel, select the device family to which your definition will apply.

The Junos OS versions and hardware platforms supported by the selected device family appear in the Description panel on the right. The OS version that appears on the lower left is the one that is set as default for that device family.



NOTE: Unless you include it in the definition name or description, the operator will not know which device family this definition applies to.

5. Select the appropriate OS version from the drop-down list in the lower part of the left panel.



NOTE: If you do not use the latest DMI schema, you will not have access to all the most recent device configuration options.

6. Click **Next**.

The second Create Definition page appears.

Creating Configuration Pages

Create configuration pages to organize and group the device configuration parameters you include in your device template definition.

The second Create Definition page displays the selected device family, the Available Configuration panel, and the Selected Configuration Layout panel.

1. In the Name box, enter a name for the template definition (limit of 63 characters).

Do not input any leading or trailing spaces. If you do, an error icon appears next to the field, and mousing over the icon displays a tooltip explaining that leading or trailing spaces are not permitted.

Each template definition must have a unique name.

2. (Optional) Enter a description in the Description box (limit of 255 characters).

The operators who use the template definition to create templates rely on the description for information on the definition.

3. In the Available Configuration panel on the left, select from the View All Configuration drop down list any of the following:

- View All Configuration—For all configuration options available for the selected device family's default DMI schema.

- Common Configuration—For the parameters typically configured for the selected device family; for example, for J/M/MX/T/TX, these are Interfaces, Routing options, SNMP, and System.
 - MPLS Pre-staging—For the parameters necessary to configure this for the selected device family; for example, for J/M/MX/T/TX, these are Interfaces, Protocols, and Routing options.
4. Display the hierarchy of Junos OS configuration options available for the device family by clicking the plus sign to the left of **Configuration** at the top of the tree.

The hierarchy appears in the form of a list. Each item can be expanded by clicking the plus sign.

5. (Optional) To find particular configuration options, see [“Finding Configuration Options” on page 199](#).
6. A default page, Config Page 1, is available to hold your groups of configuration options. Create additional pages by clicking the green plus sign at the top of the Selected Configuration Layout panel.

A new page appears in the left panel of the Selected Configuration Layout. By default, the page is named Config Page [x].
7. (Optional) To rename a page, select it and overwrite the text in the Label field on the General tab.
8. (Optional) To enter a description to help the operator or template administrator using this definition to create a template, overwrite the word Default in the Description field.
9. (Optional) Delete a page by selecting a page in the Selected Configuration Layout panel, and clicking the red X at the top of the panel.
10. To choose configurable options, drill down through the hierarchy in the Available Configuration panel. Unless you have opened a directory, selecting it and moving it does not transfer the directory’s contents into your definition. You can select multiple options simultaneously by holding down the Ctrl key.

There are three ways to move an option from the Available Configurations panel to a page in the Selected Configuration Layout panel:

- Drag one or more options from the Available Configuration panel to the Selected Configuration Layout panel, and drop it directly onto the appropriate page in the Selected Configuration Layout panel.
- First, select the destination page in the Selected Configuration Layout panel, then the option(s) to be moved.

Click the orange arrow between the panels.

The option moves from the Available Configuration panel to the Selected Configuration Layout panel.

- First select a page in the Selected Configuration Layout panel, then double-click an option in the Available Configuration panel.

The option moves to the selected page. Note that the page does not open automatically. The minus sign to the left of an empty page changes to a plus sign if the move was successful.

Any sequence is permissible, and there is no limit on the number of options a page can hold.

You cannot put children of the same parent into different pages.

If you drill down and select a parameter deep in the hierarchy, dragging that parameter causes all the other parameters that require configuration to come with it.

Determining Editable Parameters

The template definition designer specifies not only which device parameters appear in the definition, but also which parameters can be edited by the operator when he or she creates a template. The designer also sets the defaults for the editable parameters.

The data type of an option or parameter determines the configurability of the option in the finished definition. The data type is set in the DMI schema.

[Table 30 on page 192](#) lists the data types for the configuration options, and the tabs associated with each type. The data type is determined by the DMI schema, and it also determines the method of validation and the way the parameters are displayed.

To create a useful template definition, it is helpful to determine in advance which parameters or configuration options you want your operators to be able to set themselves, which parameters are to be read-only, and which, if any, are to be hidden from the operator. The data type of an option only determines how it will be displayed.

Table 30: Data Types and Tabs

Data Types	Description	Tabs			
		General	Description	Validation	Advanced
Container	Container data type holds other data types.	*	*		
Table	Table data type displays a list of records with identical structure.	*	*	*	*
String - Key column in a table	String - Key data type identifies the uniqueness of the record in the table. If the table has a key specified, only one record with the given key could exist.	*	*	*	*
String	String data type contains character strings.	*	*	*	*
Integer [Number]	Integer [Number] data type is used to specify a numeric value without a fractional component.	*	*	*	*
Boolean	Boolean data type has two possible values: true and false. True if checked and False if unchecked.	*	*		*

Table 30: Data Types and Tabs (*continued*)

Data Types	Description	Tabs			
		General	Description	Validation	Advanced
Enumeration	Enumeration data type defines a variable to be a set of predefined constants. The variable must be equal to one of the values that have been predefined for it. Use this data type to create drop-down lists.	*	*		*
Choice	Choice data type provides a radio button. Check the radio button to use the configuration option in the template.	*	*		*

Table 31 on page 193 lists the validation parameters for the data types supporting validation.

Table 31: Data Types and Validation Parameters

Data Type	Validation Parameters		
Integer [Number]	Min Value	Max Value	
String	Min Length	Max Length	Regular Expression
Table	Min Occurrence	Max Occurrence	
String - Key column in a table	Min Length	Max Length	Regular Expression

- All configuration options of the table data type have a key column by default.
- To save the settings you enter, select another tab or option or configuration page. The Next button also saves your settings. To save the entire template definition, click **Finish**.

Filling in the General Tab

The General tab enables you to create field labels that help the operator enter correct field data. The General tab applies to both the configuration *pages* and the configuration *options* you select. Here we are dealing with the options. For certain data types, filling in the General tab is optional.

To fill in the General tab for an option,

1. In the Selected Configuration Layout pane, select a *configuration option*.
The General tab appears, displaying the default text.
2. (Optional) To rename the selected option, in the Label field, overwrite the default or existing name.



TIP: Because the configuration options lose their context when you move them out of the tree in the Available Configuration panel, consider changing the default labels to indicate to operators creating templates what these parameters are for. The default labels are ambiguous without the context of the tree. For example, there are many options called *pool*.

The Data Type box displays the selected option's data type, which determines not only the tabs displayed, but also the method of validation. For tables showing the various data types and their tabs, see [Table 30 on page 192](#) and [Table 31 on page 193](#).

3. (Optional) If the data type of an option is String, it is possible to provide the template administrator or operator a drop-down list to choose from when creating templates from this definition. To provide a drop-down list of choices, change the data type of the selected option to Enumeration by clicking the Enumeration option button in the Data Type box.

Either a box containing ready-made choices appears, or a box to contain the choices you create appears, and next to it, a green plus [+] and a red minus [-] icon.

- To create each drop-down list choice, click the green plus [+] icon
A text field appears, to the right of it an OK button, a Close button, and a red X.
- Enter text in the field (limit 255 alphanumeric characters), and click **OK** when finished.

The newly created choice appears in the box to the left of the text field.



TIP: Keep your choices short, otherwise they are hard to read when you specify the default values and or when the operator tries to select from the list. You can create up to 23 choices.

- (Optional) To delete a drop-down list choice, select it and click the red minus [-] icon.

The choice disappears from the box.

- To finish adding choices, click **Close** or the red X to the right of the text field.
4. To save your entries on the General tab, select another tab or another option, or click **Next** or **Finish**.

Either fill in the General tab as described above for each option in your configuration group, or go on to fill in the Description tab for the current option.

Filling in the Description Tab

The Description tab enables you to add descriptive text to help the operator enter the correct data. When the operator creates a template, he or she can view your description or explanation by clicking the little Information icon to the right of the parameter (in the template). A pop-up appears, displaying the content you entered in the Description field.

To fill in the Description tab:

1. In the Selected Configuration Layout pane, select a configuration option. It can be the same option for which you have just filled out the General tab, or any other option.
2. Click the Description tab to display it.
3. In the Description field, enter [additional] descriptive text for the selected configuration option, or leave the default text, if desired.
4. To save your the description, move to another tab or another option, or click **Next**.

Filling in the Validation Tab

When you define fields in which you intend the operator to enter content, you usually restrict or limit that content in order to prevent validation errors during deployment. For example, if you define a field that you label **Hostname**, you could use a regular expression to prevent the operator from entering anything other than an IP address. Another situation might be when a particular attribute allows values A/B/C/D/E, but you want templates that allow only values A/C.



TIP: Remember that the definition is just the “template of the template.” Therefore in the definition you only need to set up one Primary Resolver, for example, because it is during template creation that the number of actual instances will be determined.

The Validation tab displays the validation criteria for the selected configuration option. Not all options have Validation tabs. The validation criteria are determined by the option's data type: string, integer/number, table, container, choice, or enumeration.

For a table showing data type correlated to validation criteria, see [Table 30 on page 192](#) and [Table 31 on page 193](#).



NOTE: If values are already displayed on the validation tab, they provide the range that governs the default values you set for the definition. The operator only sees the validation criteria and their values if you supply them when you create an error message.

You do not always need to enter anything on the Validation tab. However, in certain cases, input is mandatory, for example when a hostname is to be validated.

To fill in the Validation tab:

1. In the Selected Configuration Layout pane, select a configuration option of the appropriate type. It can be the same option for which you have just filled out the General and the Description tabs, or any other option for which validation is relevant.
2. Click the **Validation** tab in the Create Template Definition page.
3. Enter the parameters for the option in the appropriate fields.

If the fields already display default values and you change them, ensure that your values do not exceed the default values.

The Regular Expression Error Message box on the Validation tab appears only if you configure an option of the string data type.

4. (Optional) For a string, in the Regular Expression field, enter a regular expression to further constrain what the operator can enter.
5. (Optional) For a string, compose an error message.

This is not a validation parameter but instead a clue to enable the operator to enter correct field data. The text you enter here is displayed when an operator enters invalid content in a template field. An error message is very helpful for ensuring that operators are successful in creating templates. You cannot enter an error message if you have not entered a regular expression.

6. To save your entries, select another tab or another option, or click **Next** or **Finish**.

Filling in the Advanced Tab

The settings on the Advanced tab determine whether:

- The operator can see the selected option or edit its values
- Device-specific values will be used for the selected option. The Device Specific checkbox only appears for options of these data types:
 - Integer
 - String
 - Boolean
 - List

To fill in the Advanced tab:

1. In the Selected Configuration Layout pane, select a configuration option. It can be the same option for which you have just filled out other tabs, or any other.

If it is not already visible, the General tab appears.

2. Select the Advanced tab.
3. Select **Editable**, **Readonly**, or **Hidden**, depending on whether the operator creating the template should see this device configuration parameter, or change it.

If you hide an option, not only will the operator not see the settings for the option, but also he or she will not see the option itself.

4. (Optional) To mark this configuration option as device-specific, click the **Device Specific** check box.

See [“Specifying Device-Specific Values in Definitions” on page 200](#) for further instructions on using CSV files for this purpose. You can use rules instead of or in addition to CSV files to specify device-specific values. See [“Working with Rules” on page 203](#) for more information on this.

5. To save your entries, select another tab or another option, or click **Next**.

Specifying Default Values for Configuration Options

If you choose not to enter default values, the operator must decide what values to enter when creating a template.

To specify default values for configuration parameters:

1. On the second Create Definition page, on the Specify default values for configuration parameters page, on the left, select one of your configuration pages.

To the right a breadcrumb of that name appears, and in the pane under that, the options you added to the page on the Create Definition page.

2. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.
3. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.



NOTE: You can activate or deactivate a configuration option only if the configuration node exists.

4. To display the fields for the default values, click **View/Configure**.

The layout of the fields on the page varies depending on the data type of the configuration option you selected. For more details, see [Table 30 on page 192](#).

5. To add a row to a table, click the plus sign (+).

The fields for the options displayed in the previous view appear. Whether the operator can edit the option values depends on the settings you made on the Advanced tab, Editable, Readonly, or Hidden.

To remove a row from a table, select the row and click the minus sign (-). To edit a table row, select the row and click the pencil icon (looks like a diagonal line).

As you drill down, successive breadcrumbs appear, with the names of the options you clicked to configure, enabling you to navigate through multiple configuration option levels. The operator also sees these breadcrumbs, and uses them to navigate.

6. Enter the data as appropriate.



TIP: To review your settings, click **Back** at the bottom of the page.

Any field that you have marked as editable can remain empty, but do not leave hidden and read-only fields empty.

If you enter an invalid value, a red exclamation mark icon appears. Click the icon to find out what the value should be. The same icon is also visible to the operator when creating a template.

Click the blue Information icon on the far right of each setting to view the explanatory or descriptive text for the operator that you entered on the Description tab.

7. (Optional) To verify what the operator sees, click **Operator View**.
8. (Optional) Add settings in the Operator View.
When you click **Designer View**, a message appears, asking “Do you want to save this draft before you leave this page?”
9. (Optional) To save the settings you made in the Operator View, click **Yes**.
10. To complete your definition, return to the designer view by clicking **Designer View**.
11. Repeat these steps as necessary to specify default values for all the parameters in your definition.
12. To complete the template definition, click **Finish**.

Related Documentation

- [Finding Configuration Options on page 199](#)
- [Specifying Device-Specific Values in Definitions on page 200](#)
- [Setting a Default DMI Schema on page 722](#)

Finding Configuration Options

There are two ways to locate particular configuration options: you can browse the list or use the search function.

To display the top level configuration options, click the plus sign [+] or expansion icon at the top of the tree in the Available Configuration pane. Many of the options contain further parameters. To display these, click on the plus sign [+] or expansion icon left of the option.

To search for a specific configuration option:

1. Click the magnifying glass icon.
The search term bar appears.
2. Enter your search term.

As soon as you enter the first three letters, the bar opens downwards, displaying the search results.

Search displays only the first ten matches for your term.



TIP: Search results appear while you are typing. You can continue typing or even delete text. Note that the cursor might not be visible in the search field if the focus is somewhere within the list of search results.

The order of the search results is not dependent on the order of those items in the Available Configuration pane. It is based on the similarity of your search term to indexed fields.

3. While the result list is still visible, select a result by:

- Using the mouse to click on it.
- Pressing the Enter key to select the first result in the list.
- Using the up and down arrow keys on the keyboard to move through the list, pressing the Enter key to select a result.

The tree in the Available Configuration pane jumps to the location of the match for the result you selected and highlights the option. The list of results disappears.

4. (Optional) To review the results that you did *not* select, either:

- Click the white arrows next to the Search box.

Click the arrow to the left to move to the result listed previous to the selected result.

Click the arrow to the right to move to the result after the selected result.

- Use the left and right arrow keys on the keyboard.

Press the arrow to the left to move to the result listed previous to the selected result.

Press the arrow to the right to move to the result after the selected result.

5. To close the search bar, click the X in the top right corner of the bar.

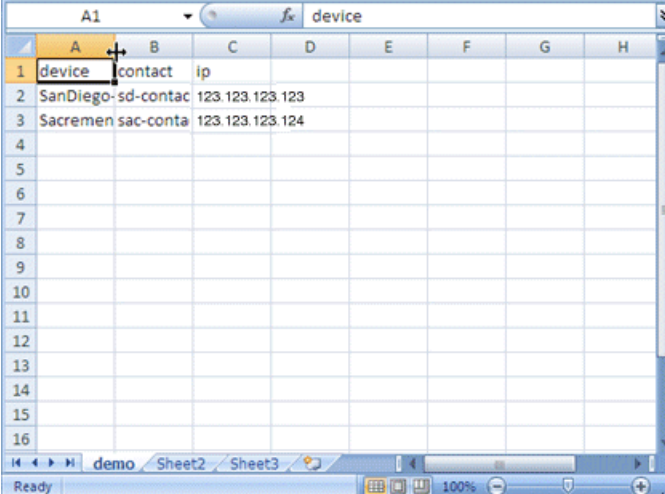
Related Documentation

- [Creating a Template Definition on page 189](#)

Specifying Device-Specific Values in Definitions

Template designers can use a comma-separated value (CSV) file to provide device-specific values for a template definition. For example, the CSV file shown in the example in [Figure 21 on page 200](#) could be used to provide the value for the SNMP contact.

Figure 21: CSV File for SNMP Contact



	A	B	C	D	E	F	G	H
1	device	contact	ip					
2	SanDiego	sd-contac	123.123.123.123					
3	Sacremen	sac-conta	123.123.123.124					
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

A single CSV file can be used to supply as many values as you wish, because the same file can be used in many situations. For example, the file shown in [Figure 21 on page 200](#) could also be used to specify IP addresses.

Once you have created a CSV file, you import it into Space, and manage it using the Manage CSV Files task in the Device Templates workspace.

To create a CSV file for use in Space, use any appropriate program such as Notepad or Excel

1. For each value to be specified, use one column.
2. For each device, use one row.
3. Create a header row to name your columns.

It does not matter what you name your columns - you could call them anything, but each name must be unique, because Space uses them to identify the values for the template definition.

In the example illustrated in [Figure 21 on page 200](#), if you wanted the value **sac-contact** in your definition, you would need to specify the column **Contact**, while the key column would be **Sacramento**.

If you wanted to specify interfaces and other values, you would simply add a column for each type of value, as in [Table 32 on page 201](#), which specifies two interfaces on a single device, as well as MTU and traps for each:



NOTE: You must correctly identify the column from which the value is to be taken and the key column when you select the CSV file during the template definition creation process. You do not necessarily need to note down this information, because you can view the contents of the CSV file in Space when you choose column and key column.

Table 32: CSV File for Interfaces

device	interface-1	mtu-1	traps-1	interface-2	mtu-2	traps-2
gemini-re0	ge-0/1/1	1514	1	ge-0/1/2	1518	0

To use a CSV file to set device-specific values in a template definition:

1. Select **Device Templates > Definitions >** and click the Create Template Definition icon.
The Create Template Definition page appears.
2. Add the configuration option for which you want to supply device-specific values using a CSV file that you have already created (see [“Managing CSV Files” on page 204](#)).
3. Click the **Advanced** tab.
4. Select the **Device Specific** check box.
5. Click **Next**.

You see the device-specific value link immediately if it is not buried, for example in a table. If you find the link immediately in the next screen, skip to Step 6. In the example illustrated in Step 4, note that the Device Specific check box applies to the Operation configuration option, which is a child of the MIB profile. Therefore clicking the Next button shows only a link for configuring the MIB profile, as shown.

To see the device-specific value link, drill down into the MIB profile by clicking **Click to Configure**.

This reveals the table where the Operation option appears (on the far right of the screen capture) as a column heading, along with the other children of the MIB profile.

In the example illustrated, you must click the **Add** button above the table to display the Device Specific Value link next to the Operation label.

6. Click the **Device Specific Value** link.

Where the device-specific value is in a table, as in the example illustrated, you must confirm that you want to add a row to the table. Click **Yes**.

The Device Specific Value [name of selected configuration option] dialog box appears.

7. Select the **Resolve the value from a CSV file at deploy time** check box.
8. Click **Please select a CSV file**.

The Manage CSV files dialog box appears.

Use the Manage CSV files dialog box to either select a file already in the system, or to navigate and upload CSV files from the local file system. You can view the content of a CSV file already in the system by selecting it in the left pane. Its content displays in the right pane.

9. To upload a file not already in the system, follow the procedure described in ["Managing CSV Files" on page 204](#).

or

To use a CSV file already in the system, select it and click **OK**.

The Device Specific Value [name of selected configuration option] dialog box reappears, this time displaying the name of the CSV file you selected in the previous steps, and the name of the configuration option whose value is to be specified by the CSV file

10. Specify the column and the key column in the CSV file.
 - a. For **Column** select the column with the value to be used. You could begin by specifying any of the values, but we will specify the *name of the first interface*: you would select **interface-1**, and for **Key Column** you would select **gemini-re0**. These specify the value **ge-0/1/1**.
 - b. Still in the Device Specific Value [name of selected configuration option] dialog box, click **Save**.

The Create Definition / Specify default values for configuration parameters page reappears.

11. Continue with Specifying Default Values for Configuration Options in [“Creating a Template Definition” on page 189](#).

**Related
Documentation**

- [Creating a Template Overview on page 222](#)
- [Deploying a Device Template on page 213](#)

Working with Rules

Device Templates uses rules to supplement the device-specific value capability supplied by CSV files. Specify rules to resolve device specific values at the time of deployment.

You can use rules in addition to CSV files, or instead of CSV files.

The system resolves device specific values by first checking the CSV file and then the rules. If both the CSV file and the rules return a value, the CSV file takes precedence. If neither the CSV file nor the rules return a value, deployment validation will fail. If a rule cannot provide the requisite value, the operator will be prompted to enter it at deployment.

Rules are applied in the order shown. You can change the order as necessary.

You can create rules for devices whose names start with a specific word, or rules for devices with a specific tag.

For the selected configuration option, on the Advanced tab, select the **Device Specific Value** check box.

You can add, edit, move, and delete rules.

You can only select one rule at a time. If no rule is selected, only the **Add** button is enabled.

To add a rule:

1. In the Device Specific Value dialog, select the check box to the left of Specify rules to resolve the value at deploy time.

The rules section of the dialog is activated, displaying the name of the configuration option for which you are setting a device specific value.

2. Click the [+] icon.

Two options appear:

- Rule matching tagged device
- Rule matching device name.

3. Select the appropriate option.

A rule appears, depending on your selection in the previous step, either of the following:

- Set to a specific value for devices tagged with a specific tag
- Set to a specific value for devices with name starting with a specific word.

In both cases, the phrase “a specific value” is a link, as are “a specific tag” and “a specific word.”

4. Click either **a specific tag** or **a specific value**.

The **Set \$dsv** field appears.

5. Enter the appropriate value.

If the value you enter is not valid, an error message appears in the form of a tool tip explaining why the entry is invalid.

6. To save your input, click the **OK** button. To clear your input, click the [X] button.

The rule reappears, this time with your input replacing the link.

7. (Optional) To change the sequence of in which the rules will be applied, select a rule and click either the up arrow icon or the down arrow icon.

The selected rule moves to the new position.

8. (Optional) To delete a rule, select the rule and click the [X] button.

The selected rule disappears.

9. (Optional) To clone a rule, select the rule and click the last icon on the right, next to the down arrow.

A clone of the selected rule appears.

10. (Optional) Refresh the rules display by clicking the Refresh icon in the lower bar of the Rules section of the Device Specific Value dialog.

11. When you have finished working with rules, close the Device Specific Value dialog box by clicking **Close**.

Related Documentation

- [Managing Template Definitions on page 183](#)
- [Creating a Template Overview on page 222](#)

Manage CSV Files

- [Managing CSV Files on page 204](#)

Managing CSV Files

Device Templates uses CSV files to specify device-specific values, in addition to rules (see “[Working with Rules](#)” on page 203). The Managing CSV Files task describes how to import this type of CSV file into Space. For instructions on the procedure for linking the file to a definition and identifying the key column for Device Templates, see “[Specifying Device-Specific Values in Definitions](#)” on page 200.

Although designers can configure the parameter governed by the CSV file as editable, operators can neither view nor change the file when they create templates.

The CSV files you use can be any file format (for example, .xls or .txt) as long as they have appropriate columns and key columns. That means one row per device. If you want

to reference several interfaces on a single device, then each of the interfaces must have its own column.

You can add a record to a CSV file from within Device Templates. However, if you change a CSV file outside Junos Space Network Management Platform, from its native application (for example, Microsoft Excel or Notepad), you must upload it again. You can do this within the device templates workflow.

To add the CSV files you use for template definitions to Junos Space Network Management Platform:

1. Select **Device Templates > Definitions** and click the Manage CSV Files icon.

The Manage CSV Files page appears.

2. Click **Upload**.

The CSV File upload dialog appears.

3. Click **Browse**.

The File Upload dialog opens.

4. Navigate to the desired CSV file, select it and click **Open**.

The CSV File upload dialog reappears, this time displaying the name of the selected file.

5. Click **Upload**.

The Manage CSV Files page reappears. The name of the file just imported appears in the left pane.

To display the content of a file, select its name in the left pane. Its content displays in the right pane.

To use the file you just uploaded, either follow the sequence of tasks in [“Creating a Template Definition Overview” on page 188](#) or go directly to [“Specifying Device-Specific Values in Definitions” on page 200](#).

Related Documentation

- [Managing Template Definitions on page 183](#)
- [Creating a Template Overview on page 222](#)

Import Definitions

- [Importing Template Definitions Overview on page 205](#)
- [Importing a Template Definition on page 206](#)

Importing Template Definitions Overview

The Import Definition facility in Device Templates enables you to import template definitions from XML files and export template definitions to XML files. You can therefore send definitions to other parties and or transfer definitions from one Junos Space fabric to another.

A definition retains its state when it is exported or imported: published definitions that are exported also appear as published when they are imported. Therefore, if you import a definition that was published, but do not want it to be available to operators, you must unpublish it either before you export it or immediately after importing it.

**Related
Documentation**

- [Exporting a Template Definition on page 187](#)
- [Importing a Template Definition on page 206](#)
- [Publishing and Unpublishing a Template Definition on page 184](#)
- [Managing Template Definitions on page 183](#)

Importing a Template Definition

Importing a template definition enables you to transfer a definition from another Junos Space fabric.

A template definition is based on a specific OS version, or DMI schema. If the definition you import is based on a schema that is not found, the definition is set to the default DMI schema assigned to the device family to which the definition applies. If you have not set default schemas for your device families, Junos Space Network Management Platform defaults to the most recent schema for each.

Before you begin, make sure you have access to a template definition file. Although it is an XML file, the system expects to find it packed into a .tgz file, which is the way the system exports .XML files (see [“Exporting a Template Definition” on page 187](#)).

To import a template definition:

1. Select **Device Templates > Definitions**.

The Definitions dialog appears.

2. Select **Import Template Definitions** from the Actions menu.
3. To locate a definition file, click the **Browse** button.

The File Upload dialog box opens.

4. Navigate to the appropriate file, select it, and click **Open**.

The Import Definition dialog box reappears, displaying the name of the selected file in the Definition File box.



.....

NOTE: Under some circumstances, when the Import Definition dialog box reappears, it displays a message beginning the phrase “Confirm name mapping of”. This message serves as a warning that the system has changed:

- The name mapping on the CSV file associated with the imported definition.
 - The name of the definition itself.
-

5. Click **Import**.

The Manage Template Definitions page reappears, displaying the newly imported template definition.

The newly imported definition has the same name as the original definition, so you may wish to use the Modify action to rename it.

**Related
Documentation**

- [Importing Template Definitions Overview on page 205](#)
- [Exporting a Template Definition on page 187](#)
- [Modifying a Template Definition on page 185](#)
- [Managing Template Definitions on page 183](#)

CHAPTER 18

Templates

- [Manage Templates on page 209](#)
- [Create Template on page 226](#)

Manage Templates

- [Managing Templates Overview on page 209](#)
- [Deleting a Template on page 212](#)
- [Deploying a Template on page 213](#)
- [Modifying a Template on page 214](#)
- [Undeploying a Template on page 215](#)
- [Viewing Template Deployment \(Device Templates\) on page 217](#)
- [Auditing Template Configuration on page 219](#)
- [Assigning a Template to a Device on page 220](#)
- [Unassigning a Template From a Device on page 221](#)
- [Creating a Template Overview on page 222](#)
- [Creating a Template on page 223](#)
- [Viewing Template Inventory on page 225](#)
- [Viewing Template Statistics on page 226](#)

Managing Templates Overview

The **Templates** page gives you access to the entire template workflow.

The **Templates inventory** page enables you to view the Junos OS device templates created to deploy configuration changes to multiple Juniper Networks discovered devices simultaneously. Device templates are created on the basis of template definitions. The designer who creates the definitions can assign the template operator settings to configure, review, or validate as necessary. The template operator then deploys the templates.




Device templates appear as rows in a table in tabular view.

From **Device Templates > Templates**, you can create , deploy, modify, or delete device templates.

Template States

Device templates have several states that are indicated in the State column of the table: review, disabled, and enabled—ready to deploy. The title and description tell you how to manage the device template. See [Table 33 on page 210](#).

Table 33: Device Template State Icon Indicators

State Icon	Description
	Needs Review—The device template cannot be deployed until you review it. This state is triggered by a designer modifying the definition on which the template is based. That template is then automatically moved into the Needs Review state.
	Disabled—The device template cannot be deployed. This state is triggered by the designer unpublishing the definition upon which a template is based. That template is then automatically disabled.
	Enabled—The device template can be deployed. As soon as you finish creating a template, it is enabled automatically.

Filtering and Searching Templates

You can filter the view of the device templates by state using the Device Templates statistics page. A quick way to view which templates you need to review, modify, or deploy is to click the status type in the Template Status pie chart—Disabled, Enabled, Needs Review. The Manage Templates inventory page appears filtered by the state you selected.

You can also search for templates by name using the Search box at the top-right in the Templates inventory page. If you start typing a template name in the Search box, you see the name in the Search Name list.

Device Template Detailed Information

Detailed template information in the Manage Templates inventory page is displayed in table columns. [Table 34 on page 210](#) describes the device template detailed information.

Table 34: Descriptive Information

Information	Description
Name	Unique name for the template.
Description	Description of the device template.
Device Family	Refers to the Juniper Networks DMI Schema, for example J/M/MX/T/TX.
Last Modified By	Login name of the operator who last modified the template.
Last Update Time	Time when the template was last updated.

Table 34: Descriptive Information (*continued*)

State	Template deployment readiness: needs review, disabled, or enabled.
Template Actions	
<p>From the Manage Templates inventory page, you can perform the following actions:</p> <ul style="list-style-type: none"> • Delete Template—See “Deleting a Device Template” on page 212. • Deploy Template—See “Deploying a Device Template” on page 213. • Modify Template—See “Modifying a Device Template” on page 214. • Undeploy Template—See “Undeploying a Device Template” on page 215 • View Template Deployment—See “Viewing Template Deployment Details (Device Templates)” on page 217 • Audit Template Configuration—See “Auditing Template Configuration” on page 219 • Assign Template to Device—See “Assigning a Device Template to Devices” on page 220 • Unassign Template From Device—See “Unassigning a Device Template From Devices” on page 221 • Publish Template to CC—See <i>Publishing a Template To CC</i> • Unpublish Template from CC—See <i>Unpublishing a Template From CC</i> • Create Template—See “Creating a Template” on page 223 • Tag It—See “Tagging an Object” on page 695. • View Tags—See “Viewing Tags for a Managed Object” on page 696. • UnTag It—See “Untagging Objects” on page 697. • Clear All Selections—All selected device templates on the Manage Templates inventory page are deselected. This action works the same as the Select: None link to the left of the Search box. 	
Related Documentation	<ul style="list-style-type: none"> • Creating a Template Overview on page 222 • User Privileges in Device Templates on page 182 • Deploying a Device Template on page 213 • Modifying a Device Template on page 214 • Deleting a Device Template on page 212 • Creating a Tag on page 698 • Tagging an Object on page 695 • Viewing Tags for a Managed Object on page 696 • Untagging Objects on page 697

Deleting a Template

Deleting a device template removes it from the Junos Space Network Management Platform database.

You need to have the appropriate user privileges before undertaking this task (see [“User Privileges in Device Templates” on page 182](#)).

1. Select **Device Templates > Templates**.

The Templates inventory page appears.

2. Select the device template you want to delete and select **Delete Template** from the Actions menu.

A window appears with the **Unpublish from CC** checkbox selected by default. Leave the default setting to ensure that the template is not deployed in a consolidated configuration (CC). If the CC has gone beyond the Prepared state, removal of the template will cause the CC to revert to the Generated state .

3. Click **OK**.

The device template disappears from the Templates inventory page

Related Documentation

- [Creating a Template Overview on page 222](#)
- [Modifying a Device Template on page 214](#)
- *Publishing a Template To CC*

Deploying a Template

Deploying a device template allows the Template Administrator or operator to update the device configuration on multiple devices. Deploying a template is the second stage of creating a template. For more information about creating a template, see [“Creating a Template” on page 223](#). You can deploy a template when you create it or schedule it to deploy later.

Before deploying a template to a device, ensure that you have not assigned the template to the same device. If you assign a template to a device and use the Deploy workflow to deploy that template on the same device, although the template is deployed to the device Junos Space Network Management Platform does not reflect this managed status. The managed status of the device is shown as "Space Changed" in the Device Management page.



NOTE: When you select devices in a service order selection, you can select devices that are down. This is permitted because the device status could change between the time the deploy is submitted and the time the actual push is performed.

Junos Space Network Management Platform allows you to validate the template against the device family and against the device.

To deploy a device template:

1. Select **Device Templates > Templates**.

The Templates inventory page appears.

2. Select the template you want to deploy and select **Deploy Template** from the Actions menu.
3. Select the devices to which you want to deploy the template.
4. Click **Next**.

The Review Changes page appears for you to review the validation result.

This is the static template validation related to the CSV file. Does the CSV file have all the device specific values? If there is an error, request that the designer fix the CSV file or ensure that the right devices have been selected to deploy the template.

The validation ensures that the template is syntactically correct against the device family.

5. Click **Validate** to test the template against the selected device.

The device validation ensures that the template is semantically correct. Junos Space Network Management Platform performs a check on the device and displays any errors in the Device Validation Result dialog box, which lists all the devices that are affected.

6. If the device validation result is successful, click **OK**.

7. Click **Next**.

The Deployment Confirmation dialog box appears.

You can select the deployment options, including scheduling deployment at a later time.

If you schedule deployment at a later time, set the time and date.

If you do not schedule template deployment, the template deploys immediately.

8. Click **Finish**.

Junos Space Network Management Platform creates a job. The Deploy Template Job Information dialog box appears.

9. Click the **job ID** to ensure the template deployment is successful.

10. Click **OK**.

11. If you need to troubleshoot template deployment, see [“Viewing Template Deployment Details \(Device Templates\)” on page 217](#). You can also navigate to **Audit Logs > Audit Log** to review what configuration was deployed on each device.

The Audit Log page captures all template deployment operations.



NOTE: If you deploy the template when in SSOR mode, Junos Space Network Management Platform automatically assigns the template to the device. To subsequently modify the template, use one of the following workflows:

- Unassign the template from the device, modify the template, and deploy the template using the **Deploy** workflow.
 - Modify the template and approve and deploy the template on the device using the **Review/Deploy Configuration** workflow in the Devices workspace.
-

Related Documentation

- [Creating a Template Overview on page 222](#)
- [Creating a Template on page 223](#)
- [Modifying a Device Template on page 214](#)
- [Deleting a Device Template on page 212](#)
- [Viewing Template Deployment Details \(Device Templates\) on page 217](#)
- [Undeploying a Device Template on page 215](#)

Modifying a Template

Modifying a device template allows you to make changes to it before deploying.

If you need to modify the template after deployment, the Template Designer must check the template and the template definition to fix any errors. Thereafter, you must redeploy the template. For more information about deploying a template, see [“Deploying a Device Template” on page 213](#).

You must have the appropriate user privileges before undertaking this task (see [“User Privileges in Device Templates” on page 182](#)).

A device template must be enabled for you to modify or deploy it.

To modify a device template:

1. Select **Device Templates > Templates**.

The Templates inventory page appears.

2. Select the device template you want to modify and select **Modify Template** from the Actions menu.
3. Modify the template name, description, or configuration settings.
4. Click **Finish**.

Now, you can deploy the template.

If you need to modify the template after deployment, the Template Designer must check the template and the template definition to fix any errors. Thereafter, you must redeploy the template. For more information about deploying a template, see [“Deploying a Device Template” on page 213](#)

Related Documentation

- [Creating a Template Overview on page 222](#)
- [Creating a Template on page 223](#)
- [Deploying a Device Template on page 213](#)
- [Deleting a Device Template on page 212](#)

Undeploying a Template

Undeploying a device template allows the Template Administrator or operator to remove the template configuration on one or more devices.



NOTE: When you select devices in a service order selection, you can select devices that are down. This is permitted because the device status could change between the time the undeploy is submitted and the time the actual pull is performed.

To undeploy a device template:

1. Select **Device Templates > Templates**.

The Templates inventory page appears.

2. Select the template you want to undeploy and select **Undeploy Template** from the Actions menu.

The Templates inventory page appears, displaying the Junos Space Network Management Platform devices to which the selected template was deployed.

3. Select the devices from which you want to undeploy the template.
4. Click **Next**.

The Review Changes page appears for you to review the configuration changes that would result from undeploying the template from the selected device(s). This page displays the information listed in [Table 35 on page 216](#)

Table 35: Review Changes Page

Device Name	Column heading: name(s) of the device(s) to which the template was deployed.
Device Specific Value	Column heading: name of configuration option to which device-specific values were applied (see “Specifying Device-Specific Values in Definitions” on page 200).
Audit Result	Column heading: displays the last audit result..
Change Summary	Tab: displays the summary of changes that will result from undeployment.
Deployed	Tab: displays the configuration pushed to the device via Template Deploy.
Audit Result	Tab: displays in sync, not in sync, or unavailable.

5. To view the Change Summary for a device, click on the name of a device in the table on the left of the Review Changes page.

The Change Summary tab appears on the right, displaying any changes resulting from the undeployment.

To view the device's current configuration, click the Deployed tab.

To view the audit of the deployment of the current template to the device, click the Audit Result tab.

6. To validate the changed configuration directly on the device, on the Change Summary tab, click **Validate on Device**.

The device validation ensures that the template is semantically correct. Junos Space Network Management Platform performs a check on the device and displays any errors in the Device Validation Result dialog box, which lists all the devices that are affected.

7. If the device validation result is successful, click **OK**.

8. Click **Next**.

The Undeployment Confirmation dialog box appears.

You can select the undeployment options, including scheduling deployment at a later time.

If you schedule undeployment at a later time, set the time and date.

If you do not schedule template deployment, the template undeploys immediately.

9. Click **Finish**.

Junos Space Network Management Platform creates a job. The Deploy Template Job Information dialog box appears.

10. Click the **job ID** to ensure the template deployment is successful.
11. Click **OK**.
12. If you need to troubleshoot template deployment, see [“Viewing Template Deployment Details \(Device Templates\)” on page 217](#). You can also navigate to **Platform > Audit Logs > View Audit Logs** to review what configuration was deployed on each device.

The Audit Log page captures all template undeployment operations.

Related Documentation

- [Deploying a Device Template on page 213](#)
- [Viewing Template Deployment Details \(Device Templates\) on page 217](#)
- [Auditing Template Configuration on page 219](#)
- [Modifying a Device Template on page 214](#)
- [Deleting a Device Template on page 212](#)

Viewing Template Deployment (Device Templates)

Viewing template deployment enables you to find out which devices a template has been deployed to, the version of the template that was deployed to each device, and to find out whether the device was in sync with the template at the time the last audit was performed, as well as other relevant details.

To get this information, you must perform an audit at least once after deploying a template. To ensure the information presented to you is current, perform a template configuration audit immediately before viewing template deployment. If there are any differences between template and device since the template was deployed.

To view the list of devices on which a template is deployed:

1. Select **Device Templates > Templates**.

The Templates page appears.

2. Select the template whose deployment you want to view.
3. Choose **View Template Deployment** from the Actions menu.

The View Deployment page appears. It shows the information described in [Table 36 on page 217](#)

Table 36: View Deployment Table

Column Header	Description
Name	Name of the device(s) to which the template is deployed.
IP Address	IP address of the device(s) to which the template is deployed.
Template Version	Version of the template currently deployed to the device named in this row.

Table 36: View Deployment Table (*continued*)

Deploy Time	Time at which the template was deployed to the device named in this row.
Deployed By	Login ID of the person who deployed the template to the device named in this row.
Job ID	ID of the job constituted by deployment of this template to the device named in this row.
Audit Status	Unavailable, in sync or not in sync.
Audit Time	Time at which the template was deployed to the device named in this row.

4. To view details of a device to which the template was deployed, double-click on the device name or its IP address
The Device Details window appears.
5. To view the change summary represented by a template version, click the number of the template version.
The Template Change Summary window appears, showing the configuration options that were changed due to the configuration snippet being deployed to the device.
6. To view the status of the job represented by deployment of the template, click the job ID.
The Job Management window appears.
7. To view any differences between a template and the configuration on the devices to which it has been deployed, first ensure an audit has been performed on the template since it was deployed (see [“Auditing Template Configuration” on page 219](#)).



NOTE: To view current information, audit the template configuration immediately before doing this: see [“Auditing Template Configuration” on page 219](#).



NOTE: Each audit is performed as a job. It may take some time to finish auditing, if a large number of devices were selected for auditing.

The possible states for a template audit are displayed in the Audit Status column:

- **Insync**
- **Out of sync**
- **Unavailable**—The Unavailable status is when no audit is performed on a device for a particular template. See [“Auditing Template Configuration” on page 219](#).

To view the audit status, click the link for the device in the Audit Status column.

The Template Audit Result window appears.

Under the Audit Status heading, any differences found last time the template was audited are listed. Such differences will be due to someone having altered the device configuration between the two template deployments.

8. To return to the Templates page from the View Deployment page, click **Cancel**.

**Related
Documentation**

- [Managing Templates Overview on page 209](#)
- [Auditing Template Configuration on page 219](#)
- [Undeploying a Device Template on page 215](#)

Auditing Template Configuration

To verify the extent to which a template and the device to which it has been deployed match, start by using the audit template configuration action. The audit can be performed immediately or scheduled for a particular time. Performing this action immediately before you view template deployment ensures that you see current information.

To view any differences between a template and the configuration on the devices to which it has been deployed,

1. Select the template whose deployment you want to audit.
2. Select **Audit Template Config** from the Actions menu,
The Audit Template Configuration window appears.
3. Select either **Audit Now** or **Audit Later**. If you select **Audit Later**, you must select the date and time by clicking the list boxes.
4. Click **Confirm**.

The Audit Template Config Information window appears.

5. To view details about the time of deployment, etc., click the job ID.
The Job Management page appears.
6. To view the audit status, click either **Insync** or **Out of sync** under the column heading Audit Status.

The Template Audit Result window appears. If Out Of Sync, it does not display the differences. It just indicates that the configuration is not the same.



NOTE: Template audit is performed on all the devices associated with the template. We do not have the option to select individual devices that are associated with the template for audit.

**Related
Documentation**

- [Managing Templates Overview on page 209](#)
- [Viewing Template Deployment Details \(Device Templates\) on page 217](#)
- [Undeploying a Device Template on page 215](#)

Assigning a Template to a Device

Assigning a template to a device enables you set up the template for deployment without actually deploying it or scheduling it for deployment. Assigning a template enables you to put the template into a queue for the device, so that all the accumulated configuration changes waiting in the queue for the device can be reviewed before any of them are deployed.



NOTE: A template that has been assigned to a device cannot be deployed directly. An assigned template becomes part of a consolidated configuration.

To assign a template to a device:

1. Select **Device Templates > Templates**.

The Templates page appears.

2. Select the template to be assigned, and select **Assign to Device** from the Actions menu.

The Assign to Device page appears.

3. Either

- Select from the table the device to which the template is to be assigned,

or

- Search for the device using the Search field at the top of the page. You can either:

- Enter the name of the device in the Search field

or

- Select the device name from a list of search results. To do this, either:

- Start entering the name of the device so that all the devices whose names begin the same way are displayed in a list.

or

- Click the magnifying glass search icon to display a list of device names.

Select the device.

4. Click **Next**.

The Confirm Assignment page appears, displaying the name of the device you selected in the last step.

5. (Optional) To make this assignment visible to others, select the **Publish changes in Consolidated Config** check box. The template assignment will then appear when the View Assigned Shared Objects action is performed on the device, and it will also appear when a consolidated config is generated.



NOTE: If you do not select the **Publish changes in Consolidated Config** check box, the template does not become available for deployment by others, even as part of a consolidated configuration. To deploy such a template, the creator of an unpublished assignment must generate his or her own consolidated config.

6. To confirm the assignment of this template to this device, click **Finish**.

The Template Assign Confirmation window appears.

7. To dismiss the Template Assign Confirmation window, click **OK**.

The Assign to Device page reappears.

Once you have assigned a template to a device, you can proceed toward deploying the template by generating a consolidated configuration (see *Managing Consolidated Configurations*).

Related Documentation

- [Viewing Assigned Shared Objects on page 68](#)
- [Publishing a Template To CC](#)
- [Unpublishing a Template From CC](#)

Unassigning a Template From a Device

Unassigning a template from a device enables you to remove the template from the device so that it is not considered for deployment. Unassigning a template enables you to remove the template from the queue for the device, so that it can no longer become part of a consolidated configuration. Unassigning unpublishes changes from Consolidated Configuration.

To unassign a template from a device:

1. Select **Device Templates > Templates**.

The Templates page appears.

2. Select the template to be unassigned, and select **Unassign to Device** from the Actions menu.

The Unassign from Device page appears, displaying a table containing the devices to which it was assigned.

3. Either

- Select from the table the devices from which the template is to be unassigned,

or

- Search for the devices using the Search field at the top of the page. You can either:

- Enter the name of the device in the Search field

or

- Select the device name from a list of search results. To do this, either:
 - Start entering the name of the device so that all the devices whose names begin the same way are displayed in a list.

or

- Click the magnifying glass search icon to display a list of device names.

Select the device.

4. Click **Next**.

The Confirm Unassignment page appears, displaying the name of the device(s) you selected in the last step.

5. To confirm the unassignment of this template to this device, click **Finish**.

The Template Unassign Confirmation window appears.

6. To dismiss the Template Assign Confirmation window, click **OK**.

The Assign to Device page reappears.

**Related
Documentation**

- [Assigning a Device Template to Devices on page 220](#)
- [Viewing Assigned Shared Objects on page 68](#)

Creating a Template Overview

Device templates enable you to update the configuration committed on multiple Juniper Networks devices in one mechanism. Deploying device templates from Junos Space Network Management Platform saves time and reduces the risk of errors, especially when you are responsible for updating the configuration on a large number of devices in the same network when many of the configuration parameters are the same.

The Junos Space Network Management Platform device templates user interface is based upon Juniper Network device family schemas. The Device Management Interface (DMI) enables Junos Space Network Management Platform to connect with and configure Juniper Networks devices.

This topic covers template creation. Template definitions must be available before you can create any templates.

Ensure that you have the appropriate user permissions before undertaking any of these tasks (see [“User Privileges in Device Templates” on page 182](#)).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in Device Templates pages.

**Related
Documentation**

- [Creating a Template on page 223](#)
- [Deploying a Device Template on page 213](#)

Creating a Template

Device templates enable operators to update the Junos OS configuration running on multiple Juniper Networks devices at once. Operators can create and deploy device templates (based on definitions created by designers) from Platform > Device Templates > Manage Templates.

Before you begin, ensure that you have the appropriate permissions (see [“User Privileges in Device Templates” on page 182](#)).

1. [Selecting a Template Definition on page 223](#)
2. [Naming and Describing a Template on page 223](#)
3. [Entering Data and Finishing the Template on page 224](#)
4. [Deploying the Template on page 225](#)

Selecting a Template Definition

The Select Template Definitions inventory page enables you to select a template definition from which to create a device template.

You can view the details of the template definition by clicking the **Details** button on each definition icon in the image view, or by looking at the grid view.

Operators cannot create or change template definitions, only templates themselves. You can regard the device template as an instance of a template definition. You can only make changes to the configuration parameters in your template if the designer has made them editable.

To select a template definition:

1. Select **Device Templates > Templates** and select the Create Template icon.
2. Select a template definition.



TIP: Operators can only see published definitions. If you do not see a definition that you expect to see, the designer might have unpublished it.

3. Click **Next**.

The Create Template page appears.

Naming and Describing a Template

The Create Templates page enables you to view the definition content so that you can name and describe the template you will create from it.

To name and describe a device template:

1. On the Create Templates page, in the Template Name box, enter a name for the device template.

The template name is required. The template name must be unique and limited to 63 characters.

2. Enter a template description in the Description box.

The template description is optional and limited to 255 characters.

If you leave a required field empty, an error message prompts you to fix the error.

Entering Data and Finishing the Template

In your template, you can see only the parameters that the definition designer has made visible. You can edit only the parameters that the definition designer has made editable. If you are looking at a template that is in the Needs Review state, it is necessary to look at all the visible parameters, whether you can change them or not.

1. In the Create Template page, on the left, select a configuration page.

To the right a breadcrumb of that name appears, and in the pane under that, the configuration options.



TIP: To navigate through the configuration options on any page, click the breadcrumbs.

As you drill down, successive breadcrumbs appear, with the names of the options you clicked to configure, enabling you to navigate through multiple configuration option levels.

The layout of the configuration settings on the page varies depending on the data type of the configuration option selected.

2. To display the settings that are not immediately evident, click **Click To Configure**.
3. (Optional) For information on the individual parameters, click the little blue information icons to the right of the configuration settings to display the explanations the designer wrote.
4. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.
5. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.



NOTE: You can activate or deactivate a configuration option only if the configuration node exists.

6. (Optional) Add any required configuration specifics.

You can change only configuration options that the definition designer made editable.



NOTE: You must click through all the settings to ensure that all necessary values are populated.

7. (Optional) To add a row to a table, click the plus sign (+).

To remove a row from a table, select the row and click the minus sign (-). To edit a table row, select the row and click the pencil icon (looks like a diagonal line).

8. Enter the data, as appropriate.

If you enter an invalid value, a red exclamation mark icon appears. Click the icon to find out what the value should be.

As appropriate, click the Undo and Redo icons to the right of the fields.

9. Click **Finish**.

The template appears on the Manage Templates inventory page. The template details include the name, description, device family, last modified by login name, last update time, and state. The template is automatically enabled.

Deploying the Template

To deploy a device template to selected devices, see [“Deploying a Device Template” on page 213](#).

Related Documentation

- [Deploying a Device Template on page 213](#)
- [Modifying a Device Template on page 214](#)
- [Publishing and Unpublishing a Template Definition on page 184](#)

Viewing Template Inventory

To view Device Template inventory, in the Device Templates workspace, click **Templates**. The Templates inventory page appears.

You can display templates in tabular view. You can also do the following:

- Use the Search function to find a particular template.
- Select all templates on a page, or you can deselect them.
- You can refresh the page by clicking the Refresh icon in the status bar.
- When you have selected a template, you can perform actions on it by right-clicking it or hovering over the Actions menu.

Related Documentation

- [Deleting a Device Template on page 212](#)
- [Deploying a Device Template on page 213](#)
- [Modifying a Device Template on page 214](#)
- [Tagging an Object on page 695](#)

- [Untagging Objects on page 697](#)
- [Viewing Device Template Statistics on page 226](#)

Viewing Template Statistics

The device template statistics page shows the states of both definitions and templates, and the number of templates per device family.

All the charts are interactive. clicking the enabled templates part of the Template Status chart, for example, takes you directly to the page displaying that category of template.



NOTE: Do not use your browser's Back and Forward buttons to navigate in Device Templates pages.

The Device Templates statistics page displays the following information:

- **Template Status**—this pie chart shows the templates that are enabled, disabled, and needing review. The templates based on a definition that is currently in a published state are enabled. Templates based on a definition that is currently unpublished are disabled. Templates based on a republished definition are marked as needing review.
- **Template Definition Status**—this pie chart shows published and unpublished definitions (available for template creation and unavailable, respectively).
- **Template Count by Device Family**—this bar chart shows the number of templates per device family (each template can apply to only one device family).

Related Documentation

- [Changing Template Definition States on page 182](#)
- [Viewing Template Inventory on page 225](#)
- [Managing Template Definitions on page 183](#)
- [Publishing and Unpublishing a Template Definition on page 184](#)

Create Template

- [Creating a Template Overview on page 227](#)
- [Creating a Template on page 227](#)

Creating a Template Overview

Device templates enable you to update the configuration committed on multiple Juniper Networks devices in one mechanism. Deploying device templates from Junos Space Network Management Platform saves time and reduces the risk of errors, especially when you are responsible for updating the configuration on a large number of devices in the same network when many of the configuration parameters are the same.

The Junos Space Network Management Platform device templates user interface is based upon Juniper Network device family schemas. The Device Management Interface (DMI) enables Junos Space Network Management Platform to connect with and configure Juniper Networks devices.

This topic covers template creation. Template definitions must be available before you can create any templates.

Ensure that you have the appropriate user permissions before undertaking any of these tasks (see [“User Privileges in Device Templates” on page 182](#)).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in Device Templates pages.

Related Documentation

- [Creating a Template on page 223](#)
- [Deploying a Device Template on page 213](#)

Creating a Template

Device templates enable operators to update the Junos OS configuration running on multiple Juniper Networks devices at once. Operators can create and deploy device templates (based on definitions created by designers) from Platform > Device Templates > Manage Templates.

Before you begin, ensure that you have the appropriate permissions (see [“User Privileges in Device Templates” on page 182](#)).

1. [Selecting a Template Definition on page 227](#)
2. [Naming and Describing a Template on page 228](#)
3. [Entering Data and Finishing the Template on page 229](#)
4. [Deploying the Template on page 230](#)

Selecting a Template Definition

The Select Template Definitions inventory page enables you to select a template definition from which to create a device template.

You can view the details of the template definition by clicking the **Details** button on each definition icon in the image view, or by looking at the grid view.

Operators cannot create or change template definitions, only templates themselves. You can regard the device template as an instance of a template definition. You can only make changes to the configuration parameters in your template if the designer has made them editable.

To select a template definition:

1. Select **Device Templates > Templates** and select the Create Template icon.
2. Select a template definition.



TIP: Operators can only see published definitions. If you do not see a definition that you expect to see, the designer might have unpublished it.

3. Click **Next**.

The Create Template page appears.

Naming and Describing a Template

The Create Templates page enables you to view the definition content so that you can name and describe the template you will create from it.

To name and describe a device template:

1. On the Create Templates page, in the Template Name box, enter a name for the device template.

The template name is required. The template name must be unique and limited to 63 characters.

2. Enter a template description in the Description box.

The template description is optional and limited to 255 characters.

If you leave a required field empty, an error message prompts you to fix the error.

Entering Data and Finishing the Template

In your template, you can see only the parameters that the definition designer has made visible. You can edit only the parameters that the definition designer has made editable. If you are looking at a template that is in the Needs Review state, it is necessary to look at all the visible parameters, whether you can change them or not.

1. In the Create Template page, on the left, select a configuration page.

To the right a breadcrumb of that name appears, and in the pane under that, the configuration options.



TIP: To navigate through the configuration options on any page, click the breadcrumbs.

As you drill down, successive breadcrumbs appear, with the names of the options you clicked to configure, enabling you to navigate through multiple configuration option levels.

The layout of the configuration settings on the page varies depending on the data type of the configuration option selected.

2. To display the settings that are not immediately evident, click **Click To Configure**.
3. (Optional) For information on the individual parameters, click the little blue information icons to the right of the configuration settings to display the explanations the designer wrote.
4. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.
5. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.



NOTE: You can activate or deactivate a configuration option only if the configuration node exists.

6. (Optional) Add any required configuration specifics.

You can change only configuration options that the definition designer made editable.



NOTE: You must click through all the settings to ensure that all necessary values are populated.

7. (Optional) To add a row to a table, click the plus sign (+).

To remove a row from a table, select the row and click the minus sign (-). To edit a table row, select the row and click the pencil icon (looks like a diagonal line).

8. Enter the data, as appropriate.

If you enter an invalid value, a red exclamation mark icon appears. Click the icon to find out what the value should be.

As appropriate, click the Undo and Redo icons to the right of the fields.

9. Click **Finish**.

The template appears on the Manage Templates inventory page. The template details include the name, description, device family, last modified by login name, last update time, and state. The template is automatically enabled.

[Deploying the Template](#)

To deploy a device template to selected devices, see [“Deploying a Device Template” on page 213](#).

**Related
Documentation**

- [Deploying a Device Template on page 213](#)
- [Modifying a Device Template on page 214](#)
- [Publishing and Unpublishing a Template Definition on page 184](#)

PART 4

CLI Configlets

- [CLI Configlets Overview on page 233](#)
- [Managing CLI Configlets on page 243](#)
- [Configuration Views Overview on page 255](#)
- [Managing Configuration Views on page 261](#)
- [XPath and Regex on page 265](#)

CHAPTER 19

CLI Configlets Overview

- [CLI Configlets Overview on page 233](#)

CLI Configlets Overview

- [CLI Configlets Overview on page 233](#)
- [CLI Configlets Workflow on page 235](#)
- [Configlets User Roles on page 237](#)
- [Configlet Context on page 238](#)
- [Nesting Parameters on page 242](#)

CLI Configlets Overview

Configlets are configuration tools provided by Junos OS that enables the user to apply configuration onto the device by reducing configuration complexity. Configlet is a configuration template which is transformed to CLI configuration string before being applied to a device. The dynamic elements (strings) in configuration templates are defined using template variables. These variables act as an input to the process of transformation, to construct the CLI configuration string. These variables can contain anything; it can be the interface name, device name, description text or any such dynamic values. The value of these variables are either got from the user, system or given by the context at the time of execution.

Velocity templates (VTL) are used to define configlets.

Configlet Workspace can be accessed by selecting CLI Configlets from the left navigation. From the configlets work space the following tasks can be performed:

- Viewing the statistics of the CLI configlets present in Junos Space Network Management Platform.
- Creating, modifying, cloning, applying, or deleting a CLI configlet.

Apart from the configlet workspace, CLI configlets can be applied from the device management workspace. It can be triggered from the actual elements for which the configuration has to be applied. The context of the element for which the configlet is being applied is called as an execution context.



NOTE: CLI Configlets are not supported on SSG Series devices, NetScreen Series devices, TCA Series devices, BXOS Series devices, and Media Flow devices.

Configlet Variables

Variables in configlets consists leading "\$". Configlets use three kinds of variables

Default Variables

The value of these variables need not be input by the user, it's taken from the current execution context. The following are the default variables.

Variable	Value
\$DEVICE	The name of the host which the configlet is being applied
\$INTERFACE	The name of the interface for which the configlet is being applied
\$UNIT	The unit number of the logical interface for which the configlet is being applied
\$CONTEXT	The context of the element for which the configlet is being applied

User defined Variables

The user provides the values for these variables at the time of execution. Text field or Selection field is used to get the value from the user.

Predefined Variables

These are the variables for which the values are predefined while creating the configlet. These are also called invisible parameters since they cannot be modified by the user.

Velocity Templates

Junos Space Network Management Platform enables the user to definite the device configuration in the form of Velocity Templates. These templates are called configlets. Configlets are transformed into CLI configuration before being applied to the device, this transformation is directed by references and directives of VTL.

References are used to embed dynamic content in the configuration text and directives allow dynamic manipulation of the content.

Please refer <http://velocity.apache.org/engine/devel/user-guide.html> for detailed documentation on VTL. VTL variable is a type of reference and consists of a leading "\$" character followed by a VTL Identifier.

Related Documentation

- [Managing CLI Configlets on page 243](#)
- [Viewing CLI Configlet Statistics on page 247](#)

CLI Configlets Workflow

A configlet can be defined from the configlet workspace. [Table 37 on page 235](#) lists the parameters to be defined for a configlet.

Table 37: Parameters for a Configlet

Parameter	Description
Name	Name of the configlet. The Name cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.). You cannot have two configlets with the same name.
Category	The Category of the configlet. The Category cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).
Device Family Series	The device family series which the configlet will be applicable for.
Context	The context for which the configlet would be applicable for. This is an optional field.
Description	Description of the configlet. The description cannot exceed 2500 characters. This is an optional field.
Preview options	Selecting the Show Parameters option displays the parameters that are present in the configlet. The Show Configuration option displays the consolidated configuration before applying the configlet.
Post-view options	Selecting the Show Parameters option displays the parameters that are present in the configlet. The Show Configuration option displays the consolidated configuration after applying the configlet.
Configlet Content	The actual configlet is defined here. The configlet can contain multiple pages and follows a tab like structure. The configuration being applied onto the device can be split among multiple pages, while applying the configuration in all the pages would be combined together in order of the page numbers and applied onto the device as a single commit operation. A configlet is always validated before moving to the next screen.



NOTE: You cannot move to the next screen if the configlet content is invalid. Validation involves bracket matching.

Parameters are the variables defined in the configlet whose values are either got from the environment or given by the user during execution. Parameters appear in the second step in the create/edit CLI configlet wizard. All the variables provided in the configlet except default variables are listed in this page initially.

To configure a parameter, click the modify icon on the toolbar. The Edit Configlet Parameter screen appears. The attributes of a parameter are set from this screen.

To add an additional parameter, click the add icon on the tool bar. The Add Configlet Parameter screen appears. The attributes of a parameter are set from this screen.

To delete a parameter, click the delete icon on the toolbar. By default, all the variables present in the configlet are listed in the parameters page. However, the local variables have to be deleted manually.

Table 2 lists the attributes of the configlet parameters.

Configlet Parameter Attributes	Description
Parameter	This field contains name of the parameter.
Display Nam	Display name of the parameter.
Description	Description of the parameter.
Types	<p>The three kinds of parameters supported are:</p> <ul style="list-style-type: none"> • Text field – You can give a custom value. A text field is shown to get the value of this field from the user while executing the configlet. The default value for this field can either be configured with an XPath in the field Configured Value XPath or with a plain string in the field Default Value. This returns a single value. • Selection field – You can select a value from a set of options. A selection field is shown to get the value of this field from the user while executing this configlet. The default value for this field can either be configured with an XPath in the field Configured Value XPath or with a plain string in the field Default Value. The options can be configured by an XPath in the field Selection Values XPath, or by a csv string in the field Selection Values. This returns a single value. <p>NOTE: Though this returns a single value, the return value is of array type and the selected value can be taken from index 0.</p> • Invisible field – You cannot edit this field. This parameter refers to a values either defined explicitly as a csv string in the field Default Value field or by an XPath in the field Configured Value XPath. This field returns an array of values.
Configured Value XPATH	<p>This field is used to give the XPath of the configured values. The behavior of this field depends on the type of parameter. When the parameter type is text field or selection field, the corresponding value present in the XPath is taken as the default value. This value can be modified. In case the XPath returns multiple values, the first value returned is considered. When the parameter type is invisible field, then the list of values returned by the XPath is taken as the value of the parameter.</p> <p>. Invisible field will have configured & selection value xpath only when the parameter scope is either device/entity specific, it will be disabled for global.</p> <p>NOTE: When using \$INTERFACE, \$UNIT, Configured Value Xpath, Invisible Params, Selection fields; the variable definition in the configlet editor should contain .get(0) inorder to fetch the value from the array. Eg: \$INTERFACE.get(0)</p>

Configlet Parameter Attributes	Description
Default Value	The behavior is same as that of Configured value XPath except that the value is given explicitly. This field is considered only when Configured Value XPATH is not specified or if the XPath doesn't return any value.
Selection Values XPATH	This field is enabled only for parameter type Selection Field. This field contains the XPath (with reference to device xml) to fetch the set of values for the selection field.
Selection Values	<p>This field is same as Selection values XPath except that the value is given explicitly. This field is considered only when Selection Values XPATH is not specified or if the XPath doesn't return any value.</p> <p>NOTE: : Comma separated values can be used in order to provide an array of values in the Default Value and Selection values field.</p> <p>NOTE: While defining the XPath, the text node has to be directly accessed with text() function. Otherwise it will return the complete xml of the node. An example would be /device/interface-information/physical-interface/name/text() to fetch the names of all interfaces.</p>
Order	The order of the parameter. The relative order in which the field has to be displayed while getting input at the time of execution.
Regex Value	This field contains the regular expression for the parameter which is used to validate the parameter value while applying the configlet to the device.

- Related Documentation**
- [Managing CLI Configlets on page 243](#)
 - [Viewing CLI Configlet Statistics on page 247](#)

Configlets User Roles

The Junos Space User Administrator is a role assigned to a Junos Space administrator that enables the administrator to grant or deny access to different Junos Space tasks. The Junos Space administrator creates users and assigns roles (permissions) so that you can access and perform different tasks. You cannot view the pages that you do not have access to. You can create users and manage them on the Manage Users page if you have User Administrator permissions. To create and manage these users, navigate to **Application Selector > Network Management Platform > Users > Manage Users**. The Manage Users page lists the existing users. Use this page to create and assign roles to the Configlets users.

[Table 38 on page 237](#) describes the Configlets tasks that different users have access to, based on the roles assigned to them.

Table 38: Configlets User Roles Permissions

User Role	Permitted Tasks
CLI Configlets Manager	Viewing, creating, modifying, cloning, deleting, applying configlets.

Table 38: Configlets User Roles Permissions (*continued*)

User Role	Permitted Tasks
CLI Configlets Operator	Applying CLI configlets.

- Related Documentation**
- [Managing CLI Configlets on page 243](#)
 - [Viewing CLI Configlet Statistics on page 247](#)

Configlet Context

For CIM and CTM, there is a need to have an ability to restrict script/configlet execution to certain elements of interest. For example, one might need to restrict the scope of execution of 'disable interface' script to just the interfaces that are enabled. Having a context associated to the script/configlet solves this problem of restricting the scope of them. Context of an element is basically a unique path which leads to its XML counterpart in the DeviceXML.

For all context related computations, we consolidate the XMLs fetched from the device under one node namely 'device', this includes configuration xml, interface-information xml, chassis-inventory xml and system-information xml.

The device xml looks like

```
<device>
  <interface-information>.....</interface-information>
  <system-information>.....</system-information>
  <chassis-inventory>.....</chassis-inventory>
  <configuration>....</configuration>
  ....
</device>
```

The following are the commands to view the XML from CLI.

XML type	Command
Chassis Inventory	> show chassis hardware display xml
Interface Information	> show interfaces display xml
Configuration	> show configuration display xml
System Information	



NOTE: The command for system information xml is not available. An instance of system information xml is given below,

```
<system-information>
<hardware-model>ex4200-24t</hardware-model>
<os-name>junos-ex</os-name>
<os-version>11.3R2.4</os-version>
<serial-number>ABCDE12345</serial-number>
<host-name>ex-device1</host-name>
<virtual-chassis/>
</system-information>
```

Context of an Element

Context of an element is the XPath that maps to the XML node that represents the element in the device xml. The Context takes the following form for each type of element

Element Type	XML referred	Context pattern
Device	N/A	/device
Physical Inventory element	Chassis Inventory	/device/chassis-inventory/*
Physical Interface	Interface Information	/device/interface-information/*
Logical Interface	Configuration	/device/configuration/*

Examples:

Element	Context	Description
Device	/device	The context of a device
Chassis	/device/chassis-inventory/chassis[name='Chassis']	Context of a chassis
Routing Engine	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='Routing Engine 0']	The context of a routing engine
FPC	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='FPC 1']	The context of an FPC in slot 1
PIC	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='FPC 1']/chassis-sub-module[name='PIC 4']	The context of a PIC in slot 4 under FPC in slot 1
Logical Interfaces	device/configuration/interfaces/interface[name='ge-0/0/1']/unit[name='0']	The context of logical interface ge-0/0/1.0

Element	Context	Description
Physical Interfaces	/device/interface-information/physical-interface[name='ge-0/1/1']	The context of a physical interface ge-0/1/1

Context filtering

The context attribute of the script/configlet dictates which elements (inventory component/logical interface/physical interface) they are applicable to.

The rule to check whether the script/configlet is applicable to an element is as follows

- Evaluate the context XPath associated to a script/configlet on the device XML. This results in a set of xml nodes.
- If the resultant xml node list contains the xml node representing the subject element, then the script/template entity is applicable for it and not applicable otherwise.

Given below are few examples of script or configlet contexts with their descriptions:

- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'Routing Engine')] - Applicable to all routing engines
- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')] - Applicable to all FPCs
- /device[starts-with(system-information/os-version,"11")]/interface-information/physical-interface[starts-with(name,"ge")] - Applicable to all interfaces of type 'ge' which has system os-version as 11
- /device/interface-information/physical-interface[admin-status="up"] - Applicable to all physical interfaces with admin status in up state.
- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')]/chassis-sub-module[starts-with(name,'PIC')] | /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')]/chassis-sub-module[starts-with(name,'MIC')]/chassis-sub-sub-module[starts-with(name,'PIC')] - Applicable to all PICs



NOTE: If we intend to specify the scope of a script as PIC's, then we would have to consider two different XPaths the PIC can take (One with MIC in-between and one without). We have to give an OR combination of both the XPaths.



NOTE: If no context is associated to a script/configlet, then the context of the script is taken as “/device”. These scripts/configlets would be listed for execution for devices.

Example

Consider the following device XML

```
<device>
  <interface-information>
    <physical-interface>
      <name>ge-0/0/0</name>
      <admin-status>up</admin-status>
      ....
    </physical-interface>
    <physical-interface>
      <name>ge-0/0/1</name>
      <admin-status>down</admin-status>
      ....
    </physical-interface>
    ....
  </interface-information>
  ....
  <!-- ALL THE OTHER NODES -->
  ....
</device>
```

Context of an element

Context of physical-interface ge-0/0/0 is

/device/interface-information/physical-interface[name='ge-0/0/0']

This XPath maps to the below node. This is the XML counterpart of the interface ge-0/0/0

```
<physical-interface>
  <name>ge-0/0/0</name>
  <admin-status>up</admin-status>
  ....
</physical-interface>
```

Context of a script/configlet

If the user wants to write a configlet to set the admin status of an interface down if its up, the context of the script can be set as

/device/interface-information/physical-interface[admin-status='up']

This configlet will be enabled only for interfaces with admin status up. Since in our example, ge-0/0/0 satisfies the above condition, this configlet can be executed on the same.

- Related Documentation**
- [CLI Configlets Overview on page 233](#)
 - [CLI Configlets Workflow on page 235](#)

Nesting Parameters

You can use XPath context to define the default option/selectable options of a parameter. This XPath could have dependencies on other parameters. Consider the example below. A configlet requires two inputs, a Physical Interface (Input-1) and a Logical Interface (Input-2) that is a part of the selected Physical Interface(Input-1). We define a parameter PHYINT to get the name of the physical interface and a parameter LOGINT to get the name of the logical interface. We define the SELECTIONVALUESXPath for PHYINT as `"/device/interface-information/physical-interface/name/text()"`. User selects a value from the options listed by the XPath. Since the selection values listed for LOGINT parameter is dependent on the value selected for PHYINT, we can define the SELECTIONVALUESXPath of LOGINT as `"/device/configuration/interfaces/interface[name='$PHYINT']/unit/name/text()"`. This ensures that, only the logical interfaces of the selected physical interface are listed.

Related Documentation

- [CLI Configlets Overview on page 233](#)

CHAPTER 20

Managing CLI Configlets

- [Manage CLI Configlets on page 243](#)
- [Viewing CLI Configlet Statistics on page 247](#)
- [CLI Configlet Examples on page 248](#)

Manage CLI Configlets

- [Managing CLI Configlets on page 243](#)

Managing CLI Configlets

You can access the Configlet page by selecting **CLI Configlets** > **Configlets** in the left navigation menu. The configlets page lists the configlets present in the system.

[Table 39 on page 243](#) describes the details on the Configlets page.

The fields Name, Category, Creation Time, Last updated time, and Last Modified By have the drop down list enabled with the filter option. This has an input field wherein you can enter the filter criteria. If you apply the filters, the table contents display only the values that match the filter criteria. The Description field does not support the filter option.

Table 39: Configlet Details

Field	Description
Name	Name of the configlet
Category	Category the configlet belongs to
Description	Description of the configlet
Creation Time	Date and time when the script was created.
Last Updated Time	Latest time when the script was last updated.
Last Modified By	Login ID of the user who last modified the configlet.

- [Creating CLI Configlets on page 244](#)
- [Viewing CLI Configlets on page 245](#)

- [Editing CLI Configlets on page 245](#)
- [Cloning CLI Configlets on page 245](#)
- [Deleting CLI Configlets on page 246](#)
- [Applying CLI Configlets on page 246](#)

Creating CLI Configlets

To create a configlet:

1. Select **CLI Configlets > Configlets > Create CLI Configlet**.
The Create CLI Configlet page appears.
2. Enter the necessary parameters.
3. Click **Next** to view the Parameters page.

[Table 40 on page 244](#) describes the information on the Parameters page.

Table 40: Parameters Page

Field	Description
Parameter	The name of the parameter as used in the configlet
Display Name	User friendly name for the parameter
Description	Description of the parameter
Parameter Type	Type of the parameter. It can take one of the following values: <ul style="list-style-type: none"> • Text Field – User can give his own value. • Selection Field – User can select a value from a set of options. • Invisible Field – This parameter refers to a value either defined explicitly or by an XPath.
Configured Value XPath	This field specifies the XPath (With reference to device XML), from which the value of the parameter has to be fetched. In case of Selection field and invisible field, this is the default value and cannot be modified.
Default Value	The behavior is same as that of Configured value Xpath except that the value is given explicitly. This field is considered only when XPath is not specified.
Selection Values Xpath	This field is enabled only for parameter type Selection Field. This field contains the XPath (with reference to device xml) to fetch the set of values for the selection field.
Selection Values	This field is same as Selection values XPath except that the comma separated value is given explicitly.
Order	The order in which the parameters would be listed while applying.

The parameters are auto populated along with the display name, parameter type and order onto this screen based on the configlet content provided earlier. All the variables

used in the configlet definition except default variables are listed here. These parameters can be configured.

4. Click **Create** to create the configlet.

Viewing CLI Configlets

To view details of a CLI configlet:

1. Select **CLI Configlets > Configlets**.

The Configlets page displays the configlets in a table.

2. Select a configlet whose details you want to view.
3. From the Actions menu, select **View CLI Configlet**.

The View CLI Configlet window appears. The details of the configlet can be viewed from this window.

4. Click **Close** to go back to the Configlets page.

Editing CLI Configlets

To edit a CLI configlet:

1. Select **CLI Configlets > Configlets**.

The Configlets page displays the configlets in a table.

2. Select the configlet you want to edit.
3. From the Actions menu, select **Edit CLI Configlet**.

The Edit CLI Configlet page appears. Modify the necessary parameters.

4. Click **Update** to save your changes and go to the configlets page.

Cloning CLI Configlets

To clone a CLI configlet:

1. Select **CLI Configlets > Configlets**.

The Configlets page displays the configlets in a table.

2. Select the configlet you want to clone.
3. From the Actions menu, select **Clone CLI Configlet**.

The Clone CLI Configlet page appears.

4. Click **Create** to save your changes and go to the configlets page.

Deleting CLI Configlets

To delete a CLI configlet:

1. Select **CLI Configlets > Configlets**.

The Configlets page displays the configlets in a table.

2. Select the configlet you want to delete.
3. From the Actions menu, select **Delete CLI Configlet**.

The Delete Operations dialog box lists the operations that you chose for deletion.

4. Click **Confirm** to delete the configlet.

Applying CLI Configlets

To apply a CLI configlet on a device from the Configlets page:

1. Select **CLI Configlets > Configlets**.

The Configlets page displays the configlets in a table.

2. Select the configlet you want to apply to a device.
3. Right click the selected configlet in the table and select **Apply CLI Configlet**.

The Apply CLI Configlet page appears.

4. Select the device that you want to apply the configlet on.
5. Enter the values for the parameters. (Only text field and selection field are displayed)

To view the description of the parameter hover the mouse pointer over the entry in the Parameter column.

In a text field, the user can enter any value while for a selection field, the user can select one of the values from a given set. The set of values present and the default value selected are all defined while creating a template.

6. Click **Next**.

The preview of the configlet appears. The preview page displays the parameters and the configuration being applied.



NOTE: The information displayed in the preview page depends on the preview options selected during creation of the configlet.

7. Click **Validate** to perform the configuration validation check. This step is optional.

The Validate configlet dialog box appears, asking that you wait while the configuration is being validated. When it has finished, the device validation status appears, announcing success or failure.

8. Click **Apply** to apply the configuration.

The apply CLI configlet job results window appears. The Results page displays the parameters and the configuration that was applied.



NOTE: The information displayed in the Results page depends on the postview options selected during creation of the configlet.

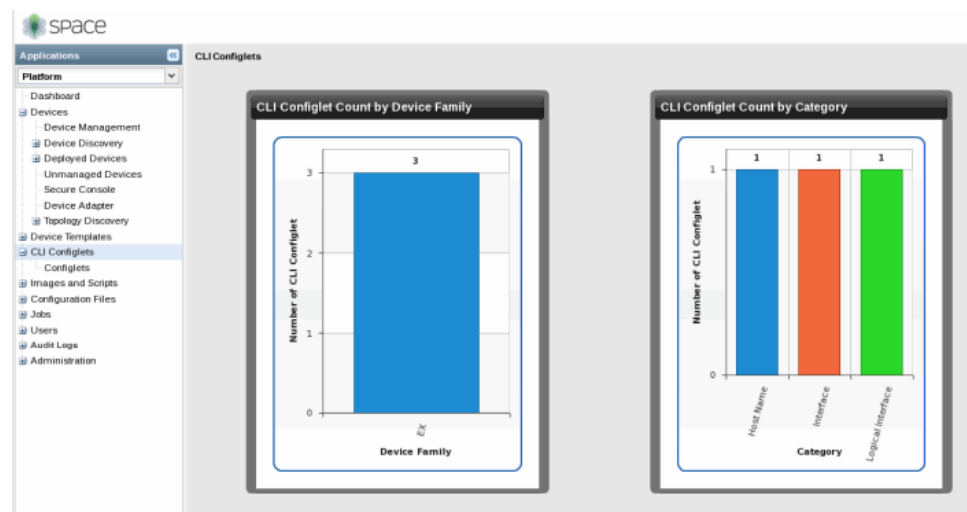
9. Close the window to go back to Configlets page.

- Related Documentation**
- [CLI Configlets Overview on page 233](#)
 - [Viewing CLI Configlet Statistics on page 247](#)

Viewing CLI Configlet Statistics

The configlets statistics page provides two types of data for the configlets. – CLI configlet count by device family, and the CLI configlet count by category. CLI configlet count by device provides the number of configlets applicable to the respective device family. CLI configlet count by category provides the number of configlets belonging to the respective categories. To view configlets statistics, select **Platform > CLI Configlets**.

Figure 22: CLI Configlets Statistics



Viewing the Number of Configlets by Device Family

The bar chart shows the number of Configlets on the y axis and device family series on the x axis.

To view more detailed information about configlets per device family, click a bar in the bar graph. The configlets page appears filtered by the device family type you selected.

To save the bar chart as an image or to print for presentations or reporting, right click the bar chart and use the menu to save or print the image.

Viewing the Number of Configlets by Category

The bar chart shows the number of Configlets on the y axis and category on the x axis.

To view more detailed information about configlets per category, click a bar in the bar graph. The configlets page appears filtered by the category you selected.

To save the bar chart as an image or to print for presentations or reporting, right click the bar chart and use the menu to save or print the image.

Related Documentation

- [CLI Configlets Overview on page 233](#)

CLI Configlet Examples

- [CLI Configlet Examples on page 248](#)

CLI Configlet Examples

Example 1 - Setting the description of a physical interface

Context: /device/interface-information/physical-interface This configlet is targeted for physical interface

Configlet:

```
interfaces {
  $INTERFACE{
    description "$DESC";
  }
}
```

Parameters

Parameter	Details
\$INTERFACE	This is a default variable and the value would be the name of the interface which the configlet is invoked from. This would be null if the configlet is invoked from configlet workspace as the execution is not associated a specific interface.
\$DESC	A text field to get the description string. The value is got at the time of execution.

On Applying the configlet, the user needs to input the parameters. For our example, user needs to input a value for \$DESC.

Consider our example being applied to an interface ge-0/1/3 and the following values are given as input.

Parameter	Value
\$DESC	TEST DESC

The generated configuration string would be

```
interfaces {
  ge-0/1/3{
    description "TEST DESC";
  }
}
```

Example 2 - Setting the vlan of a logical interface, where the vlan id is chosen from a predefined set of values

Context: /device/configuration/interfaces/interface/unit This configlet is targeted for logical interface

Configlet

```
interfaces {
  $INTERFACE {
    vlan-tagging;
    unit $UNIT{
      vlan-id $VLANID.get(0);
    }
  }
}
```

##Since VLAN id will be given as a selection field, the value would be a collection and to get the first selected value, use .get(0)

Parameter	Details
\$INTERFACE	This is a default variable and the value would be the name of the interface which the configlet is invoked from. This would be null if the configlet is invoked from configlet workspace as the execution is not associated a specific interface.
\$UNIT	This is a default variable and the value would be the unit name of the logical interface which the configlet is invoked from. This would be null if the configlet is invoked from configlet workspace as the execution is not associated a specific logical interface.
\$VLANID	<p>This is a selection field and the value would be chosen at the time of execution.</p> <p>Type: Selection Field</p> <p>Selection Values: 0,1,2,3</p> <p>Default Value: 3</p>

On applying the configlet, the user needs to input the parameters. For our example, user needs to input a value for \$VLANID.

Consider our example being applied to an interface ge-0/1/3.3 and the following values are given as input.



NOTE: Since \$VLANID is defined as a selection field, the user has to select one values form a list. The list of options are either specified by Selection Values Xpath or in Selection Values field. The default selection in the list would be 3 as defined in the default value field.

Parameter	Value
\$VLANID	2

The generated configuration string would be

```
interfaces {
  ge-0/1/3 {
    vlan-tagging;
    unit 3 {
      vlan-id 2;
    }
  }
}
```

Example 3 - Setting a description on all the interfaces of a device

Context: NULL or /device. Targeted to a device, the context of a device can either be null or /device

Configlet

```
interfaces {
  #foreach($INTERFACENAME in $INTERFACENAMES)
  $INTERFACENAME {
    description "$DESC";
  }
  #end
}
```

Parameter	Details
\$INTERFACENAMES	An invisible variable with an XPath configured to fetch all the interface names. Configured values XPath: /device/interface-information/physical-interface/name/text()
\$DESC	A text field to get the description string. The value is got at the time of execution.

The following input is given while executing the configlet

Parameter	Value
\$DESC	TEST DESC

The generated configuration string would be (when the device has three physical interfaces, ge-0/0/0, ge-0/0/1 and ge-0/0/2).

```
interfaces {
  ge-0/0/0 {
    description "TEST DESC";
  }
  ge-0/0/1 {
    description "TEST DESC";
  }
  ge-0/0/2 {
    description "TEST DESC";
  }
}
```

Example 4 - Need to set a configuration in all the PICs belonging to a device and certain configuration only on the first PIC of FPC 0

Context: NULL or /device. Targeted to a device, the context of a device can either be null or /device

##\$ELEMENTS :

/device/chassis-inventory/chassis/chassis-module[starts-with(name,"FPC")]

/name/text() | /device/chassis-inventory/chassis/chassis-module

[starts-with(name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]/name/text()

##this will contain the list of all FPCs and PICs in Depth-first traversal order.

##Hierarchy array is a 2 dimensional array used to store FPC-PIC hierarchy, with each row containing PICs belonging to a single FPC, The first element is the FPC.

Configlet

```
#set( $HIERARCHY = [] )
#set( $LOCALARRAY = [] )
#foreach ( $ELEMENT in $ELEMENTS )
#if( $ELEMENT.startsWith("FPC"))
## Create a new array for each FPC with the first element as FPC
#set( $LOCALARRAY = [ $ELEMENT ] )
#set( $result = $HIERARCHY.add( $LOCALARRAY ) )
#elseif( $ELEMENT.startsWith("PIC"))
## Add the PIC in the current Local array, this is the array of the parent FPC
#set( $result = $LOCALARRAY.add( $ELEMENT ) )
#end
#end
chassis {
  redundancy {
    failover on-disk-failure;
    graceful-switchover;
  }
  aggregated-devices {
    ethernet {
      device-count 16;
    }
  }
}
```

```

}
foreach ($HIERARCHYELEMENT in $HIERARCHY)
$HIERARCHYELEMENT.get(0) {
#set($HIERARCHYELEMENTSIZE = $HIERARCHYELEMENT.size() - 1)
foreach ($HIERARCHYELEMENTINDEX in [1..$HIERARCHYELEMENTSIZE] )
$HIERARCHYELEMENT.get($HIERARCHYELEMENTINDEX){

## Set the tunnel services setting for the first PIC in FPC 0
#if($HIERARCHYELEMENTINDEX == 1 && $HIERARCHYELEMENT.get(0) == "FPC 0")
tunnel-services {
bandwidth 1g;
}
#end
traffic-manager {
ingress-shaping-overhead 0;
egress-shaping-overhead 0;
mode ingress-and-egress;
}
}
#end
}
#end
}
}

```

Parameters

Parameter	Details
\$ELEMENTS	<p>This is an invisible field and the value cannot be set by the user at the time of execution. The values are taken form a predefined XPath</p> <p>Type: Invisible field</p> <p>Configured Value XPath: /device/chassis-inventory/chassis/chassis-module[starts-with(name,"FPC")] /name/text()/device/chassis-inventory/chassis/chassis-module[starts-with (name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]/name/text() This XPath returns the list of FPCs and PIC is Depth First Traversal order.</p>

While executing this Configlet, the XPath of \$ELEMENTS param will return the list of FPCs and PIC present in the device. The values for instance would be [FPC 0,PIC 0,PIC 1, FPC 1, PIC 0, PIC 1] This order implies the association

FPC 0

PIC 0

PIC 1

FPC 1

PIC 0

PIC 1

When the configlet is executed, we get the following configuration string

```
chassis {
  redundancy {
    failover on-disk-failure;
    graceful-switchover;
  }
  aggregated-devices {
    ethernet {
      device-count 16;
    }
  }
}
fpc 1 {
  pic 0 {
    tunnel-services {
      bandwidth 1g;
    }
    traffic-manager {
      ingress-shaping-overhead 0;
      egress-shaping-overhead 0;
      mode ingress-and-egress;
    }
  }
  pic 1 {
    traffic-manager {
      ingress-shaping-overhead 0;
      egress-shaping-overhead 0;
      mode ingress-and-egress;
    }
  }
}
fpc 2 {
  pic 0 {
    traffic-manager {
      ingress-shaping-overhead 0;
      egress-shaping-overhead 0;
      mode ingress-and-egress;
    }
  }
  pic 1 {
    traffic-manager {
      ingress-shaping-overhead 0;
      egress-shaping-overhead 0;
      mode ingress-and-egress;
    }
  }
}
}
```

Example 5 - Halting the description of a physical interface

Context: /device/interface-information/physical-interface This configlet is targeted for physical interface

Configlet

```
interfaces {
  #if( $INTERFACENAME == 'ge-0/0/0')
  #terminate('Should not change description for ge-0/0/0 interfaces.')
  #{else}
  $INTERFACENAME {
    unit 0 {
      description "Similar desc";
      family ethernet-switching;
    }
  }
  #end
}
```

- Related Documentation**
- [CLI Configlets Overview on page 233](#)
 - [Viewing CLI Configlet Statistics on page 247](#)

CHAPTER 21

Configuration Views Overview

- [Configuration View Overview on page 255](#)
- [Configuration View Variables on page 256](#)
- [Configuration View Workflow on page 256](#)
- [Configuration Views User Roles on page 257](#)
- [XML Extensions on page 258](#)

Configuration View Overview

Configuration Views are configuration tools provided by Junos OS that enables the user who wants to see configuration details in his/her own way. Two types of configuration views are Form View and Grid View. Form View is simple view of configuration as key value pair. The dynamic fields in form view are defined using parameters. Grid view, a customizable grid that can show key(column) list of values(rows) pair. The dynamic column values in grid view are defined using parameter definitions. Velocity templates (VTL) are used to define the parameters.

Configuration Views Workspace can be accessed by selecting Configuration Views from the task bar. From the Configuration View work space the following can be performed:

- View the statistics of the Configuration Views present in Junos Space Network Management Platform.
- Create, Modify, Delete a Configuration Views.

Configuration Views can be created from the View Device Configuration workspace. It can be triggered from the actual elements for which the configuration has to be applied. The actual elements are represented in a tree structure of device configuration xml. The context of the element for which the Configuration View is being created is called execution context.

Related Documentation

- [Manage Configuration Views on page 261](#)

Configuration View Variables

A parameter name in Configuration View consists of a leading "\$". Configuration View uses three kinds of variables. Configuration views can use the following default variables to define a parameter.

Default Variables

The values of the variables are taken from the current execution context. The following are the default variables.

Variable	Value
\$DEVICE	The name of the host which the configuration view is being created
\$INTERFACE	Name of the interface for which the configuration view is being created
\$UNIT	The unit number of the logical interface for which the configuration view is being created
\$CONTEXT	The context of the element for which the configuration view is being created

Velocity Templates

Junos Space Network Management Platform enables the user to define the device configuration view parameter's XPath using Velocity Templates. Nested parameters are referred using VTL. Please refer <http://velocity.apache.org/engine/devel/user-guide.html> for detailed documentation of VTL. VTL variable is a type of reference and consists of a leading "\$" character followed by a VTL Identifier.

Related Documentation

- [Manage Configuration Views on page 261](#)

Configuration View Workflow

A configuration view can be defined from the Configuration View workspace, Configuration View will have the following parameters to be defined.

Name	Name of the configuration view. The Name cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.). You cannot have two configuration view with the same name.
Title	Title of the configuration view. The title cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).
Device Family Series	The device family series which the configuration view will be applicable for.
Context	The context for which the configuration view would be applicable for.
Description	Description of the configuration view. The description cannot exceed 2500 characters. This is an optional field.

Order	Order of the configuration view tab in Device Configuration View. Order accepts only numbers.
View Type	View types are Form View and Grid View.
<p>Parameters are the variables defined in the configuration view whose values are got from the environment. Parameters appear in the create/edit configuration view, as they are added to configuration view. To configure a parameter, click modify icon on the toolbar, the Edit Form View Parameter appears. The attributes of a parameter are set from this screen. To add additional parameter, clicks add icon on the tool bar, the Add Form View Parameter screen appears. The attributes of a parameter are set from this screen. To delete a parameter, click the delete icon on the toolbar. A parameter has the following specific attribute.</p>	
Parameter	Name of the parameter.
Index Parameter	<p>To consider a parameter as an index parameter or not. This is applicable for a grid view only. An index parameter should meet at least one of the following two conditions except when only one parameter is defined in a grid view.</p> <ul style="list-style-type: none"> • An index parameter should refer at least one of the other index parameters. • An index parameter should be referred in one of the other parameters. <p>A non index parameter should always refer at least one index parameter.</p>
Display Name	Display name of the parameter.
Configured Value XPATH	<p>This field is used to give the XPath of the configured values. The behavior of this field depends on the type of view. When the view type is form, the corresponding value present in the XPath is taken as the field value. In case XPath returns multiple values, first value returned is considered. In case the XPath returns multiple values, the first value returned is considered. When the view type is grid, the following behavior is followed. If more than one parameters defined then following rules should be met.</p> <ul style="list-style-type: none"> • For independent index parameters, a join would be performed between the values returned by the XPath and the existing set of rows. • For dependent index parameters, join would be performed between the values returned by the XPath and the correspondent row. <p>For non index parameters, if list of values returned then they are aggregated into comma separated values.</p>
Order	The order of the parameter. The relative order in which the parameter has to be displayed.

Related Documentation • [Manage Configuration Views on page 261](#)

Configuration Views User Roles

The Junos Space User Administrator is a role assigned to a Junos Space administrator that enables the administrator to grant or deny access to different Junos Space tasks. The Junos Space administrator creates users and assigns roles (permissions) so that you can access and perform different tasks. You cannot view the pages that you do not

have access to. You can create users and manage them on the Manage Users page if you have User Administrator permissions. To create and manage users, navigate to Platform > Users > User Accounts. The Manage Users page lists the existing users. Use this page to create and assign roles to the Configuration View users. The following table describes the Configuration View tasks that different users have access to, based on the role assigned to them.

User Role	Permitted Tasks
Configuration View Manager	Viewing, creating, modifying, deleting configuration views and Viewing device configuration.
Configuration View Operator	Viewing Configuration view details and device configuration details

Related Documentation

- [Manage Configuration Views on page 261](#)

XML Extensions

In configuration-view, the querying is not restricted to the Device XML data. Space lets users define parameters that can fetch additional details that are not a part of the device XML itself.

Operational Status

In the config viewer, realtime status of the component could be queried using the XPATH `<xpath-of-the-component>/oper-status`.



NOTE: For physical interface component `<xpath-of-physical-inteface>/oper-status/text()` wouldn't work. Its only possible to query with `<xpath-of-physical-inteface>>/oper-status`. This limitation doesn't apply for chassis components.

Customized Attributes

In config viewer, Custom attributes of a component could be queried using the XPATH `<xpath-of-the-component>/customized-attribute[name='<attribute-name>']`.

While defining a view with customized attribute, the user has an option to make it editable. Making a customized attribute editable would allow the user to edit the values inline. Changes would be persisted immediately. To make a customized attribute editable, enable the checkboxes 'Customized Attribute' and 'Editable'. Custom attributes are editable only in Grid View.



NOTE: For custom attributes XPATH `<xpath-of-the-component>/customized-attribute[name='<attribute-name>']` would work properly, but `/text()` or any other extensions at the end of the xpath wouldn't work.

**Related
Documentation**

- [Manage Configuration Views on page 261](#)

CHAPTER 22

Managing Configuration Views

- [Manage Configuration Views on page 261](#)
- [Viewing Configuration Views Statistics on page 263](#)

Manage Configuration Views

Configuration Views landing page can be accessed by selecting Configuration Views> Configuration View from the task bar. The configuration views landing page will list the configuration views present in the system. The following describes the information that appears on the Configuration Views page. The fields Name, Title, Creation Time, Last updated time, and Last Modified By have the drop down list enabled with the filter option, which has an input field wherein you can enter the filter criteria. On applying the filter(s), the table contents display only the values that match the filter criteria. The field Description, however, does not support the filter option.

Field	Description
Name	Name of the configuration views.
Title	Title of the configuration view
Device Family	Family of the device to which it belongs to
Description	Description of the configuration views
Order	The order in which the view has to be applied and it accepts only values > 0.
View Type	The views are Form view, Grid view, and XML view.
Creation Time	Date and time when the configuration views was created.
Last Updated Time	Latest time when the configuration views was last updated.
Last Modified By	Login ID of the user who last modified the configuration views.

You can perform the following tasks from the Configlets page:

- [Create Configuration View on page 262](#)
- [View Configuration View on page 262](#)
- [Edit Configuration View on page 263](#)
- [Delete Configuration View on page 263](#)

Create Configuration View

1. From the taskbar, select **Configuration Views > Configuration View > Create Configuration View**. The Create Configuration View page appears.

The following describes the information that appears on the parameters/columns section

Field	Description
Parameter	The name of the parameter as used in the configuration form view
Display Name	The name of the parameter as used in the configuration grid view
Script Dependent	The configuration view is dependent on any local script or not.
Local Script Name	If configuration view is dependent on any local script, its name will be mentioned.
Index Column	Index column or not.
Display Name	User friendly name for the parameter/column name.
Configured Value XPath	This field specifies the XPath (With reference to device XML), from which the value(s) of the parameter/column has to be fetched.
Customized Attribute	To associate additional data to devices, device interface and device inventory.
Editable	Either the customized attribute is editable or not.
Order	The order in which the parameters/columns would be displayed while applying.

2. Click on **Create** to create the configuration view.

View Configuration View

To view details of a Configuration View:

1. From the taskbar, select **Configuration Views > Configuration View**. The configuration view page displays the configuration view in a table.
2. Select a configuration view whose details you want to view.
3. From the Actions menu, select **View configuration view**. The View Configuration View window appears.

The details of the configuration view can be viewed from this window.

4. Click **Close** to go back to the Configuration View page.

Edit Configuration View

To modify a Configuration View:

1. From the taskbar, select **Configuration Views > Configuration View**. The configuration view page displays the configuration view in a table.
2. Select a configuration view whose details you want to edit.
3. From the Actions menu, select **Edit Configuration View**. The Edit Configuration View window appears.
4. Modify the necessary sections and click on **Update** to save your changes and go to the Configuration View page.

Delete Configuration View

You can use Junos Space Network Management Platform to delete a Configuration View from the Junos Space Network Management Platform database. To delete a Configuration View:

1. From the taskbar, select **Configuration Views > Configuration View**. The configuration view page displays the configuration view in a table.
2. Select a Configuration View you want to delete.
3. From the Actions menu, select **Delete Configuration View**. The Delete Operations dialog box lists the operations that you chose for deletion.
4. Click on **Confirm** to delete the Configuration View.

Related Documentation

- [Viewing Configuration Views Statistics on page 263](#)

Viewing Configuration Views Statistics

The configuration view statistics page provides two types of data for the configuration view.

- Configuration view count by device family – The number of configuration view applicable to the respective device family.
- Configuration view count by category – The number of configuration view belonging to the respective categories.

To view configuration view statistics, select the **Platform > Configuration Views**.

Viewing the Number of Configuration Views by device family

To view more detailed information about configuration views per device family, click a bar in the bar graph. The configuration views page appears filtered by the device family type you selected.

Figure 23: Configuration Views Chart



To view more detailed information about configuration views per category, click a bar in the bar graph. The configuration views page appears filtered by the category you selected.

Related Documentation

- [Manage Configuration Views on page 261](#)

CHAPTER 23

XPath and Regex

- [XPATH and Regex on page 265](#)
- [Creating Xpath and Regex on page 265](#)
- [Managing Xpath and Regex on page 266](#)

XPATH and Regex

While developing configlets, XPaths and Regular Expressions would be used intensively. It would be desirable to let the user define frequently used XPaths and Regular expressions in such a way that they can be referred when required. User can define these templates from 'XPath and Regex' workspace (CLIConfiglets > XPath and Regex).

Xpaths and Regular expressions defined here are referred from all the fields that require the defined type as input. The user defined values can be selected from the dropdown provided for the field. This can be edited at the field level.

Related Documentation • [Creating Xpath and Regex on page 265](#)

Creating Xpath and Regex

1. Select **Network Application Platform > CLI Configlets > Xpath and Regex**.
The Xpath and Regex page is displayed.
2. Click the Create Xpath and Regex icon on the menu bar.
The Create Xpath/Regex page is displayed.
3. In the **Name** field, enter the name of the Regex or Xpath.
4. From the **Property Type** field, select an appropriate value for the Xpath or Regex.
5. In the **Value** field, enter an appropriate value.
6. Click **Create**.

Related Documentation • [Managing Xpath and Regex on page 266](#)

Managing Xpath and Regex

You can modify or delete the Xpath and Regex.

- [Modifying the Xpath and Regex on page 266](#)
- [Deleting the Xpath and Regex on page 266](#)

Modifying the Xpath and Regex

To modify the Xpath and Regex:

1. Select **Network Application Platform > CLI Configlets > Xpath and Regex**.
The Xpath and Regex page is displayed.
2. Select the Xpath or Regex you want to modify and select the Modify icon on the menu bar.
3. Modify the Xpath or Regex properties.
4. Click **Update**.

Deleting the Xpath and Regex

To delete the Xpath and Regex:

1. Select **Network Application Platform > CLI Configlets > Xpath and Regex**.
The Xpath and Regex page is displayed.
2. Select the Xpath or Regex you want to delete and select the Delete icon on the menu bar.
The Delete Xpath/Regex pop-up window is displayed.
3. Select the Xpath or Regex you want to delete and click **Confirm**.

Related Documentation

- [Creating Xpath and Regex on page 265](#)

PART 5

Images and Scripts

- [Overview on page 269](#)
- [Device Images on page 273](#)
- [Scripts on page 275](#)
- [Operations on page 279](#)
- [Script Bundles on page 281](#)
- [Configuration: Device Images on page 283](#)
- [Configuration: Scripts on page 297](#)
- [Configuration: Operations on page 315](#)
- [Configuration: Script Bundles on page 325](#)
- [Administration: Scripts on page 335](#)
- [Administration: Operations on page 339](#)
- [Administration: Script Bundles on page 341](#)
- [Annotations and Examples on page 343](#)

CHAPTER 24

Overview

- [Device Images and Scripts Overview on page 269](#)

Device Images and Scripts Overview

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

Device Images and Scripts is a workspace in the Junos Space Network Management Platform that enables you to manage these device images and scripts.

You can access the Images and Scripts workspace by clicking **Images and Scripts** on the taskbar.

The Images and Scripts workspace enables you to perform the following tasks:

- Manage device images

You can upload device images from your local file system and deploy these device images to a device or onto multiple devices of the same device family simultaneously. After uploading device images, you can stage a device image on a device, verify the checksum, and deploy the staged image whenever required. You can also schedule the staging, deployment, and validation of device images.

- Manage scripts

You can import multiple scripts into the Junos Space server and perform various tasks such as modifying the scripts, viewing their details, exporting their content, comparing them, and deploying them on multiple devices simultaneously. After you deploy scripts onto devices, you can use Junos Space Network Management Platform to enable, disable, and execute them on those devices.

- Manage operations

You create, manage, export, import, and execute operations that combine multiple script and image tasks, such as upgrading images and deploying or executing scripts, into a single bundle for efficient use and reuse.

- Manage script bundles

You can group multiple op scripts into a script bundle. Script bundles can be deployed and executed on devices. You can also modify and delete script bundles.

User Roles

The Junos Space user administrator creates users and assigns roles (permissions) so that users can access and perform different tasks. You must be given access to a page in order to view it. While Junos Space Network Management Platform allows the admin to create users and control their access to different tasks, it also has a set of predefined user roles. [Table 41 on page 270](#) describes the Device Images and Scripts tasks to which different users have access, based on the roles the admin assigns to them.

You can create users and manage them on the Users page, if you have user administrator permissions. To create and manage these users, select **Network Management Platform** > **Users** > **User Accounts**. The Users page lists the existing users. Use this page to create and assign roles to Device Images and Scripts users.

You can enable and disable scripts on devices that use Junos Space Network Management Platform only if you are a superuser with complete permissions or a user who has been given maintenance privileges.



NOTE: The Junos OS management process executes commit scripts with root permissions, not the permission levels of the user who is committing the script. If the user has the necessary access permissions to commit the configuration, then Junos OS performs all actions of the configured commit scripts, regardless of the privileges of the user who is committing the script.

Table 41: Device Images and Scripts User Roles

User Role	Permitted Tasks
For Device Images	
Device Image Manager	Viewing, uploading, modifying, deleting, staging, verifying the checksum of, and deploying device images.
Device Script Manager	Viewing, importing, modifying, comparing, deleting, deploying, enabling, disabling, verifying, removing, and executing scripts.
For Scripts	
Device Script Read Only User	View execution results, view associated devices, compare, export scripts
Device Image Read Only User	Viewing Images pages.
Device Script Operator	Executing scripts and viewing execution results.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Operations Overview on page 279](#)

- [Scripts Overview on page 275](#)
- [Script Bundles Overview on page 281](#)

Device Images

- [Device Images Overview on page 273](#)

Device Images Overview

In Junos Space, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. You can download these device images from <https://www.juniper.net/customers/support/> . For more information about downloading the device image, see the *Junos OS Installation and Upgrade Guide*.

Junos Space Network Management Platform facilitates management of device images for devices running Junos OS by enabling you to upload device images from your local file system and deploy these device images onto a device or onto multiple devices of the same device family simultaneously. You can modify the platforms supported by the device image and the description of the device image. After uploading device images, you can stage a device image on a device, verify the checksum, and deploy the staged image whenever required. You can also schedule the staging, deployment, and validation of device images.

[Table 42 on page 273](#) describes the Images page. The fields **File Name** and **Version** have the drop down list enabled with the filter functionality, which has an input field wherein you can enter the filter criteria. On applying the filter(s), the table contents display only the values that match the filter criteria. The field **Series**, however, does not support the filter option.

Table 42: Manage Images Page

Field	Description
File Name	Name of the device image.
Version	Version of the device image.
Series	Series supported by the device image.

You can perform the following tasks from the Images page:

- Stage an image on devices
- Verify the checksum
- Deploy device images
- Delete device images
- Modify device images

**Related
Documentation**

- [Deploying Device Images on page 286](#)
- [Staging Device Images on page 284](#)
- [Modifying Device Image Details on page 294](#)
- [Uploading Device Images to Junos Space on page 283](#)
- [Scripts Overview on page 275](#)
- [Script Bundles Overview on page 281](#)
- [Operations Overview on page 279](#)

CHAPTER 26

Scripts

- [Scripts Overview on page 275](#)

Scripts Overview

Scripts are configuration and diagnostic automation tools provided by Junos OS. They help reduce network downtime and configuration complexity, automate common tasks, and decrease the time to problem resolution. Junos OS scripts are of three types: commit, op, and event scripts.

- **Commit scripts:** Commit scripts enforce custom configuration rules and can be used to automate configuration tasks, enforce consistency, prevent common mistakes, and more. Every time a new candidate configuration is committed, the active commit scripts are called and inspect the new candidate configuration. If a configuration violates your custom rules, the script can instruct the Junos OS to perform various actions, including making changes to the configuration, and generating custom, warning, and system log messages.
- **Op scripts:** Op scripts enable you to add your own commands to the operational mode CLI. They can automate the troubleshooting of known network problems, and correcting them.
- **Event scripts:** Event scripts use event policies to enable you to automate network troubleshooting by diagnosing and fixing issues, monitoring the overall status of the router, and examining errors periodically. Event scripts are similar to op scripts but are triggered by events that occur on the device.

Using Junos Space Network Management Platform you can import multiple scripts into the Junos Space server. After importing scripts, you can perform various tasks such as modifying the scripts, viewing their details, exporting their content, comparing them, viewing their association with devices and deploying them on multiple devices simultaneously. After you deploy scripts onto devices, you can use Junos Space Network Management Platform to enable, disable, and execute them on those devices. You can remove the scripts from the devices as well. To help ensure that the deployed scripts are not corrupt, you can verify the checksum of the scripts.

Junos Space Network Management Platform also supports task scheduling. You can specify the date and time when you want a script to be deployed, verified, enabled, disabled, removed, or executed.

Junos Space Network Management Platform provides an option to associate scripts to devices. It maintains this association with the information pertaining to the current status of the script. Based on this feature, Junos Space Network Management Platform supports the following operations:

- Associating scripts with devices and maintaining the association
- Displaying the status (version, enabled/disabled) of scripts on the devices
- Displaying the results of script execution on the devices
- Upgrading the scripts to the latest version on some or all the associated devices
- Auto upgrading the scripts on the associated devices, whenever the script is modified from Junos Space Network Management Platform
- Removing the script-device association



NOTE:

- You can perform script related operations (enable/disable/remove/verify/execute scripts, excluding stage scripts) only if the scripts are associated with the devices.
- If you want to delete scripts from Junos Space Network Management Platform, first remove the scripts from device, and then delete all the related associations.
- You cannot modify the script type if there is an association with a device. You need to first remove the scripts from device, and then modify the script type.

Table 43 on page 276 describes the information that appears on the Scripts page.

The fields **Script Name**, **Descriptive Name**, **Type**, **Execution Type**, **Format**, and **Latest Revision** have the drop down list enabled with the filter option, which has an input field wherein you can enter the filter criteria. On applying the filter(s), the table contents display only the values that match the filter criteria. The fields **Description**, **Creation Date**, **Last Updated Time**, and **Association** however, do not support the filter option.

Table 43: Scripts Page Fields Description

Field	Description
Script Name	Name of the script file
Descriptive Name	Descriptive name of the script
Type	Type of script: <ul style="list-style-type: none"> • Commit script • Op script • Event script

Table 43: Scripts Page Fields Description (*continued*)

Field	Description
Execution Type	<ul style="list-style-type: none"> • Devices • Local
Format	Format of the script file: <ul style="list-style-type: none"> • XSL • SLAX
Latest Revision	Latest version number of the script.
Creation Date	Date and time when the script was created.
Last Updated Time	Latest time when the script was last updated.
Associations	The associated devices for a script are displayed when you click View under Associations

You can perform the following tasks from the Scripts page:

- Import scripts
- View script details
- Modify scripts
- Modify script types
- Compare script versions
- Delete scripts
- Export scripts in .tar format
- Stage Scripts on Devices
- View Associated Devices
- View execution results
- Verify the checksum of scripts on devices
- View verification results
- Enable scripts on devices
- Disable scripts on devices
- Remove scripts from devices
- Execute scripts on devices

**Related
Documentation**

- [Device Images and Scripts Overview on page 269](#)
- [Importing Scripts on page 313](#)
- [Viewing Script Details on page 335](#)

- [Modifying a Script on page 297](#)
- [Modifying Script Types on page 298](#)
- [Comparing Script Versions on page 299](#)
- [Deleting Scripts on page 299](#)
- [Exporting Scripts in .tar Format on page 337](#)
- [Staging Scripts on Devices on page 300](#)
- [Viewing Script Execution Results](#)
- [Verifying the Checksum of Scripts on Devices on page 302](#)
- [Viewing Verification Results on page 336](#)
- [Enabling Scripts on Devices on page 304](#)
- [Disabling Scripts on Devices on page 306](#)
- [Removing Scripts from Devices on page 307](#)
- [Executing Scripts on Devices on page 309](#)
- [Device Images Overview on page 273](#)
- [Script Bundles Overview on page 281](#)
- [Operations Overview on page 279](#)
- [Viewing Device Association of Scripts on page 301](#)

CHAPTER 27

Operations

- [Operations Overview on page 279](#)

Operations Overview

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

Junos Space Network Management Platform enables you to simultaneously execute scripts and device images by allowing you to group tasks, such as staging device images and deploying or executing scripts, into a single operation. This facilitates efficient use and reuse.

Using the Operations task, you can:

- Create an operation
- Modify an operation
- Create a copy of an existing operation
- Execute (or run) an operation
- Delete an operation
- Export an operation
- Import an operation
- View information about operations in four stages of execution (successful, failed, in progress, and scheduled).

Related Documentation

- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)
- [Deleting an Operation on page 320](#)

- [Exporting an Operation in .tar Format on page 320](#)
- [Importing an Operation on page 322](#)
- [Scripts Overview on page 275](#)
- [Device Images Overview on page 273](#)
- [Script Bundles Overview on page 281](#)

CHAPTER 28

Script Bundles

- [Script Bundles Overview on page 281](#)

Script Bundles Overview

Scripts are configuration and diagnostic automation tools provided by Junos OS. They help reduce network downtime and configuration complexity, automate common tasks, and decrease the time to problem resolution. Junos OS scripts are of three types: commit, op, and event scripts.

Junos Space Network Management Platform allows you to group multiple op scripts into a script bundle. To create a script bundle, you must first import the scripts that you want to include in the script bundle (see [“Importing Scripts” on page 313](#)). The script bundles that you create are displayed on the Script Bundles page. Script bundles can be deployed and executed on devices. You can also modify and delete script bundles. For more information about scripts, see [“Scripts Overview” on page 275](#).

Based on the user role assigned to your username, Junos Space Network Management Platform enables and disables different tasks. For more information about Junos Space Network Management Platform— User roles see, [“Device Images and Scripts Overview” on page 269](#).

You can execute the following tasks from the Script Bundles page:

- Create script bundles
- Deploy script bundles to devices
- Execute script bundles on devices
- Modify a script bundle
- Delete script bundles
- Enable scripts in script bundles on devices
- Disable scripts in script bundles on devices
- View device association of scripts in script bundles

Related Documentation

- [Creating a Script Bundle on page 325](#)
- [Staging Script Bundles on Devices on page 328](#)

- [Executing Script Bundles on Devices on page 329](#)
- [Modifying a Script Bundle on page 326](#)
- [Deleting Script Bundles on page 327](#)
- [Enabling Scripts in Script Bundles on Devices on page 330](#)
- [Disabling Scripts in Script Bundles on Devices on page 332](#)
- [Viewing Device Associations of Scripts in Script Bundles on page 341](#)
- [Device Images Overview on page 273](#)
- [Scripts Overview on page 275](#)
- [Operations Overview on page 279](#)

Configuration: Device Images

- Uploading Device Images to Junos Space on page 283
- Staging Device Images on page 284
- Verifying the Checksum on page 286
- Deploying Device Images on page 286
- Viewing Device Image Deployment Results on page 293
- Deleting Device Images on page 293
- Modifying Device Image Details on page 294
- Viewing and Deleting MD5 Validation Results on page 295

Uploading Device Images to Junos Space

To deploy a device image that uses Junos Space Network Management Platform, you must first download the device image from the Juniper Networks Support webpage <http://www.juniper.net/customers/support/>. Download the device image to the local file system of your workstation or client, and then upload it into the Junos Space Network Management Platform server. After the image is uploaded, you can stage a device image, verify the checksum, deploy the device image on one or more devices, modify the description and supported platforms, and also delete the device image from Junos Space Network Management Platform.

To upload device images:

1. Select **Images and Scripts > Images** and select the **Import Image** icon.

The Import Images page appears.

2. Click **Browse**.

The File Upload dialog box displays the directories and folders on your local file system.

3. Navigate to the device image file and click **Open**.

4. Click **Upload**.

The time taken to upload the file depends on the size of the device image and the connection speed between the local machine and the Junos Space Network Management Platform server. After the file is uploaded onto the server, it is listed on the Images page.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Deploying Device Images on page 286](#)
 - [Staging Device Images on page 284](#)

Staging Device Images

Junos Space Network Management Platform enables you to stage an image on one device or on multiple devices of the same device family simultaneously. Staging an image enables you to hold a device image on a device, ready to be deployed when needed. At any given time, you can stage only a single device image. Staging images repeatedly on a device merely replaces the staged device image. While staging device images, you can also delete existing device images from the device. After you stage a device image, you can verify the checksum to ensure that the device image was transferred completely.

To stage an image on devices:

1. Select **Network Management Platform > Images and Scripts > Images**.

The Images page appears.

2. Select the selected device image and select **Stage Image on Device**. This page displays a list of the Junos Space devices.
3. Select the device or devices on which you want to stage the device image, by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled. .



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

4. To select devices manually:
 - Click the **Select by Device** option and select the device(s) on which you want to stage the device image.

The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.

 - To select all the devices, select the check box in the column header next to Host Name.
5. To select devices based on tags:
 - Click the **Select by Tags** option. The Select by tags list is activated.
 - Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.

- You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
 - Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.
6. To delete existing device images from the device, expand the **Staging Options** section and select the **Delete any existing image before download** check box. This deletes all .tgz files and files whose filenames begin with **jinstall**.
 7. To schedule a time for staging the device image, select the **Schedule at a later time** check box and use the lists to specify the date and time.
 8. Click **Stage Image**.
- The image is staged on the selected device or devices and a Jobs dialog box displays the job ID.
9. To verify the status of this job, click the job ID link or navigate to the Jobs page and view the status of the job. When there is a failure in the staging of the device image, you can view the reason for failure within the job description.

To verify the checksum of the staged device image, see [“Verifying the Checksum” on page 286](#).

Table 44: Stage Image On Devices Dialog Box Fields Descriptions

Field	Description
Image Name	Name of the device image.
Host Name	Identifier used for network communication between Junos Space Network Management Platform and the Junos OS device.
IP Address	IP address of the device.
Platform	Model number of the device.
Serial Number	Serial number of the device chassis.
Software Version	Operating system firmware version running on the device.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Deploying Device Images on page 286](#)
 - [Verifying the Checksum on page 286](#)

Verifying the Checksum

When you stage an image on a device that uses Junos Space Network Management Platform, sometimes the device image might not get completely transferred to the device. Verifying the checksum helps validate the completeness of the staged device image.

To verify the checksum:

1. Select **Network Management Platform > Images and Scripts > Images**.

The Images page appears.

2. Select the image whose checksum you want to verify.
3. Select **Verify Checksum** from the Actions menu.

The Images dialog box appears.

4. Select the devices that have the device image staged on them.
5. To schedule a time for verifying the checksum, select the **Schedule a later time** check box and use the lists to specify the date and time.
6. Click **Verify**.

The selected image is verified and a Jobs dialog box displays the job ID.

7. To check the status of verification you can click on the job ID link or navigate to the Jobs page and view the job status.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Deploying Device Images on page 286](#)

Deploying Device Images

Junos Space Network Management Platform enables you to deploy device images onto a device or on multiple devices of the same device family simultaneously. During deployment, a device image is installed on the device. After you deploy an image onto a device, you can reboot the device, delete the device image from the device, check the device image's compatibility with the current configuration of the device, and load the image when even a single statement is valid. Using an image that is already staged on a device eliminates the time taken to load the device image on a device and directly jumps to the installation process. Junos Space Network Management Platform also enables you to schedule a time when you want the image to be deployed.

On dual Routing Engine platforms, you can also do an in-service software upgrade (ISSU) between two different Junos software releases with no disruption on the control plane and with minimal disruption of traffic. This provides the following benefits:

- Eliminates network downtime during software image upgrades
- Reduces operating costs, while delivering higher service levels
- Allows fast implementation of new features.

During the ISSU, the backup Routing Engine is rebooted with the new software package and switched over to make it the new primary Routing Engine. The former primary Routing Engine can also be upgraded to the new software and rebooted.

Table 45 on page 287 describes the devices and software releases that support ISSU.

Table 45: Routing Platforms and Software Releases Supporting ISSU

Routing Platform	Software Release
M120 router	Junos 9.2 or later
M320 router	Junos 9.0 or later
MX-series Ethernet Services router	Junos 9.3 or later
NOTE: Unified ISSU for MX-series does not support IEEE 802.1ag OAM, IEEE 802.3ah, and LACP protocols.	
SRX Series Gateways	Junos 10.4R4 or later
NOTE: For more information about upgrade limitations of unified ISSU on high-end SRX Series firewalls, see the Knowledge Base article KB17946 at http://kb.juniper.net/KB17946 .	
T320 router	Junos 9.0 or later
T640 routing node	Junos 9.0 or later
T1600 routing node	Junos 9.1 or later
TX Matrix platform	Junos 9.3 or later



NOTE: EX Series switches do not support ISSU.

Additionally you must note the following in connection with doing an ISSU:

- You can upgrade to a software version that supports unified ISSU from a software version that does not support unified ISSU only by means of a conventional upgrade. During the conventional upgrade, all line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.
- The armed (upgrade) release must be capable of being upgraded to from the currently running release.
- All applications that are configured on the router must support unified ISSU and stateful SRP switchover.
- If one or more unified ISSU-challenged applications are configured and you proceed with a unified ISSU, the unified ISSU process forces a conventional upgrade on the router.
- To perform ISSU on an MX device, you must manually configure the device to enable **Non-stop bridging**, in addition to the GRES and NSR that Space enables on the dual RE device for ISSU.



NOTE: We strongly recommend that you configure the Master only IP on the dual Routing Engine device. Dual Routing Engine devices without Master only configuration are not yet fully supported on Junos Space Network Management Platform.

For complete details about the protocols, features, and PICs supported by ISSU, refer to the Unified ISSU System Requirements sections in the *Junos OS High Availability Configuration Guide*.

You can deploy a device image only onto devices or platforms supported by that device image. When you select an image for deployment, the list of the displayed devices contains only those devices that are supported by the selected device image.



NOTE: In Junos Space Network Management Platform, an SRX Series cluster is represented as two individual devices with cluster peer information. When you deploy a device image on an SRX cluster, the image is installed on both cluster nodes.



NOTE: If you want to select **Check compatibility with current configuration** for **Conventional Deploy Image** on a dual RE device, make sure that GRES and NSR are disabled on the device.

To deploy device images:

1. Select **Network Management Platform > Images and Scripts > Images**.
The Images page appears.
2. Select the image that you want to deploy.

The selected image is highlighted.

3. Select **Deploy Device Image** from the Actions menu.

The Select Devices table at the top of the Deploy Image on Device page displays the devices that are supported by the selected device image. For a description of the fields in this table, see [Table 50 on page 292](#).

4. Select the devices on which you want to deploy the device image by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

5. To select devices manually:

- Click the **Select by Device** option and select the device(s) on which you want to stage the device image.

The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.

- To select all the devices, select the check box in the column header next to Host Name.

6. To select devices based on tags:

- Click the **Select by Tags** option. The Select by tags list is activated.
- Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
- Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.

7. To select devices using a CSV file:
 - Select the radio button next to the Select by CSV button.
 - Click the **Select by CSV** button and upload the list of devices on which you want to deploy the device image.
8. To specify different deployment options, select one or more of the check boxes in the Common Deployment Options and/or Conventional Deployment Options sections.

See [Table 46 on page 291](#) and [Table 47 on page 291](#) for a description of the deployment options.



NOTE: When you do a conventional upgrade of the device image on dual Routing Engines (RE), the image is first deployed on the backup Routing Engine followed by the primary Routing Engine. If deployment fails on the backup Routing Engine, the device image is not deployed on the primary Routing Engine.

9. (Optional) To perform an ISSU on a dual Routing Engine device, open the ISSU Deployment Options section, and check one or more of the check boxes. The ISSU option is enabled only if the selected device has a dual Routing Engine. This capability is shown in the Platform column in the Select Devices table in the upper part of the screen.
- See [Table 48 on page 292](#) for a description of the ISSU deployment options.
10. To specify advanced deployment options, select one or more of the Select Advanced Deployment options check boxes. See [Table 49 on page 292](#) for a description of the advanced deployment options.

To configure the script parameters of scripts included in the script bundle:

- a. Select the prescript or postscript bundle that you want to configure, using the respective lists.

If there are no script bundles available, you can create script bundles using the Scripts workspace (see [“Creating a Script Bundle” on page 325](#)) and then re-select the script bundle during script deployment.

- b. Click the **Configure Scripts Parameters** link.

The Configure Script Bundle Parameters page appears. You can hover over the script parameters to view short descriptions about them.

- c. You can edit the value (success or failure) of script parameters using the icon shown below before deploying the script bundles on devices. The changes made to script parameters are saved only on the devices on which the script bundle is executed. The script parameters in the script bundle in Junos Space Network Management Platform continues to reflect the original values.
- d. Click **Configure**.

Your changes are saved and the Deploy Image on Device page appears.

11. To schedule a time for deployment, select the **Schedule at a later time** check box and use the lists to specify the date and time.
12. Click **Deploy**.
The selected image is deployed on the specified devices with the deployment options that you specified.
13. To view the result of deployment, navigate to the View Deploy Results page. See [“Viewing Device Image Deployment Results” on page 293](#).

Table 46: Common Deployment Options Description

Common Deployment Options	Description
Use image already downloaded to device	Use the device image that is staged on the device for deployment.
Archive Data (Snapshot)	Collect and save device data and executable areas.
Remove the package after successful installation	Delete the device image from the device after successful installation.
Delete any existing image before download	Delete all device images with the same filename from the device before deploying the selected device image.

Table 47: Conventional Deployment Options Description

Conventional Deployment Options	Description
Check compatibility with current configuration	Verify device image compatibility with the current configuration of the device.
Load succeeds if at least one statement is valid	Ensure that the device image is loaded successfully even if only one of the statements is valid.
Reboot device after successful installation	Reboot the device after deployment is successful. If the device is down, Junos Space Network Management Platform waits for the device to come up before initiating the reboot. If the device is not up within 30 minutes, the Image Deployment Job is marked as failed. After rebooting the device, the status of the device is checked every 5 minutes to check whether the device is up.
Upgrade Backup Routing Engine only	Deploys the image to only the backup Routing Engine.
Dual-Root Partitioning for SRX	Supports dual partition for SRX devices.

Table 48: ISSU Deployment Options Description

ISSU Deployment Options	Description
Upgrade the former Master with new image	After the backup Routing Engine is rebooted with the new software package and a switchover occurs to make it the new primary Routing Engine, the former primary (new backup) Routing Engine is automatically upgraded. If you do not check this option, the former primary must be manually upgraded.
Reboot the former Master after a successful installation	The former primary (new backup) Routing Engine is rebooted automatically after being upgraded to the new software. If this option is not selected, you must manually reboot the former primary (new backup) Routing Engine.
Save copies of the package files on the device	Copies of the package files are retained on the device.

Table 49 on page 292 describes the different advanced deployment options.

Table 49: Advanced Deployment Options Description

Advanced Deployment Options	Description
Execute script bundle before image deployment (pre scripts)	<p>With this option, you have the opportunity to configure scripts parameters after you have select a script bundle.</p> <p>Execute the selected script bundle before deploying the device image. This ensures that the scripts in the selected script bundle are executed before the device image is installed on the device.</p>
Select same pre script bundle for post script bundle	Execute the same script bundle on the device before and after device image deployment.
Execute script bundle after image deployment (post scripts)	<p>With this option, you have the opportunity to configure scripts parameters after you have select a script bundle.</p> <p>Execute the selected script bundle before deploying the device image. This ensures that the script bundle is executed after the device image is installed on the device.</p>
Deploy and Enable script bundle before execution	Deploy the selected script bundle, enable the scripts included in the script bundle, and then execute the script bundle on the device.
Disable scripts after execution	Execute the script bundle on the device and then disable the script bundle.

describes the **Select Devices** table fields.

Table 50: Select Devices Table Field Descriptions

Field	Description
Image Name	Name of the device image. (This field is above the table.)
Host Name	Identifier used for network communication between Junos Space Network Management Platform and the device running Junos OS.

Table 50: Select Devices Table Field Descriptions (*continued*)

Field	Description
IP Address	IP address of the device.
Platform	Model number of the device.
Serial Number	Serial number of the device chassis.
Software Version	Operating system firmware version running on the device.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Uploading Device Images to Junos Space on page 283](#)
 - [Script Bundles Overview on page 281](#)

Viewing Device Image Deployment Results

You can view the results of device image deployment and also filter these results to display only the failures in deployment.

To view deployment results:

1. Select **Images and Scripts** > **Images** and click the **View Deployed Results** icon.
The View Deployed Results page displays the job ID, timestamp, name of the image, job description, scripts executed, and the results of the device images that you deployed on devices.
2. To view only the failures in deployment, select the **Show Failures** check box.
3. Click **Images** on the left-hand side to return to the Images page.

- Related Documentation**
- [Deploying Device Images on page 286](#)
 - [Staging Device Images on page 284](#)

Deleting Device Images

You can delete device images from Junos Space Network Management Platform including deleting multiple device images simultaneously.

To delete device images from the Junos Space Network Management Platform:

1. From the taskbar, select **Network Management Platform** > **Images and Scripts** > **Images**.
The Images page appears.
2. Select the image that you want to delete.
The selected image is highlighted.

To select multiple device images, click the **Multiple** tab, and select the images you want to delete.

3. Select **Delete Device Images** from the Actions menu.

The Delete Device Image dialog box displays the image filename and the image version number.

4. Click **Delete** to confirm the deletion.

The selected image is deleted from Junos Space Network Management Platform and no longer appears on the Images page.

Related Documentation

- [Device Images Overview on page 273](#)
- [Deploying Device Images on page 286](#)
- [Staging Device Images on page 284](#)

Modifying Device Image Details

Junos Space Network Management Platform enables you to add and modify the description of a device image and also to modify the series that the device image supports.

To modify the parameters of a device image:

1. Select **Network Management Platform > Images and Scripts > Images**.

The Images page appears.

2. Select the image that you want to modify. The selected image is highlighted.

3. Select a device image and select **Modify Device Image Details**.

The Modify Device Image Details dialog box appears.

4. To modify the series, use the Series list and specify the series that the selected device image supports. The platforms that are part of the selected series are automatically displayed in the Platforms box and cannot be modified.

To add or modify the description, you can use a maximum of 256 characters within the Description box.

5. Click **Modify**.

Your changes are saved. These changes can be viewed on the device image detail and summary view.

Related Documentation

- [Device Images Overview on page 273](#)
- [Deploying Device Images on page 286](#)
- [Deleting Device Images on page 293](#)

Viewing and Deleting MD5 Validation Results

Using Junos Space Network Management Platform, you can validate completeness of a device image that is staged on devices. See [“Verifying the Checksum” on page 286](#). The result of this validation appears on the Validation Results page. From this page you can view and delete the validation results.

- [Viewing the MD5 Validation Results on page 295](#)
- [Deleting the MD5 Validation Results on page 296](#)

Viewing the MD5 Validation Results

The MD5 validation results indicate whether the device image that is staged on a device is completely transferred to the device or not. The result also indicates whether the device image is not present on the selected devices.

To view the MD5 validation results:

1. From the taskbar, select **Network Management Platform > Images and Scripts > Images**.
The Images page displays the list of device images.
2. Select a device image.
3. Select **MD5 Validation Result** from the Actions menu.

The Validation Results page displays the results of verification tasks.

[Table 51 on page 295](#) describes the Validation Results page.

Table 51: Validation Results Page Field Descriptions

Field Name	Description
Device Image Name	Name of the device image selected for verifying the checksum.
Device Name	Name of the selected devices on which the device images are verified.
Action	Name of the action performed.
Checksum Result	Result of the verification
Remarks	Observations made during the verification.
Verification Time	Time at which the verification was initiated.

Deleting the MD5 Validation Results

To delete the MD5 validation results:

1. Select **Images and Scripts > Images**.

The Images page appears.

2. Select a device image.
3. Select **MD5 Validation Result**.

The Validation Results page displays the results of all verification tasks.

4. Select the result that you want to delete.
5. Right-click your selection and select **Delete Validation Results**.

The **Delete Validation Results** dialog box displays the selected results.

6. Click **Delete** to confirm.

The selected results are removed from Junos Space Network Management Platform.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Staging Device Images on page 284](#)
 - [Verifying the Checksum on page 286](#)

CHAPTER 30

Configuration: Scripts

- [Modifying a Script on page 297](#)
- [Modifying Script Types on page 298](#)
- [Comparing Script Versions on page 299](#)
- [Deleting Scripts on page 299](#)
- [Staging Scripts on Devices on page 300](#)
- [Viewing Associated Devices on page 301](#)
- [Verifying the Checksum of Scripts on Devices on page 302](#)
- [Enabling Scripts on Devices on page 304](#)
- [Disabling Scripts on Devices on page 306](#)
- [Removing Scripts from Devices on page 307](#)
- [Executing Scripts on Devices on page 309](#)
- [Viewing Execution Results on page 311](#)
- [Importing Scripts on page 313](#)

Modifying a Script

You can use Junos Space Network Management Platform to modify the script type, script contents, and the script version to the latest version of the script. You can also add your comments to the details of a script. When you modify a script, the script is saved as the latest version by default. Junos Space Network Management Platform modifies both the associated and unassociated scripts. To modify the script type for multiple scripts, see [“Modifying Script Types” on page 298](#).

To modify a script:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the script that you want to modify.
3. Select **Modify Script** from the Actions menu.

The **Modify Script** dialog box displays the details of the script.

4. You can modify the script type, script contents, and the comments about the script. Script type will be disabled if it is associated to any device.

5. Click **Next**.

The **Modify Scripts** page displays a list of all the associated device(s) that are preselected. You can deselect the device(s) for which the script need not be upgraded with the current modification. The script is modified immediately and upgrade step alone can be scheduled.

6. Click **Finish**. The **Scripts** page appears.

Your changes are saved to the latest version of the script, and the old version of the script is retained. Junos Space Network Management Platform updates the Latest Revision column and it now displays the latest version of the script.

7. To verify these changes, you can view the details of this script. See [“Viewing Script Details” on page 335](#).

The **Latest Version** column displays the latest version.

8. Click **Cancel** to withdraw your changes and return to the **Scripts** page.

- Related Documentation**
- [Staging Scripts on Devices on page 300](#)
 - [Scripts Overview on page 275](#)

Modifying Script Types

Using Junos Space Network Management Platform, you can modify the script type of multiple scripts simultaneously.

To modify the script type:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The **Scripts** page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the script whose script type you want to modify.

3. Select **Modify Scripts Type** from the Actions menu.

The **Modify Scripts Type** dialog box displays the details of the script.

4. Use the Bulk Actions list to select a common script type for all scripts. To modify script types of individual scripts, click the **Script Type** column heading and use the drop-down menu to make your changes.

5. Click **Apply**.

Your changes are saved and the Manage Scripts page appears.

6. (Optional) To verify, double-click the script that you modified and view the script type.

- Related Documentation**
- [Viewing Script Details on page 335](#)
 - [Staging Scripts on Devices on page 300](#)

Comparing Script Versions

Using Junos Space Network Management Platform you can compare two scripts and view their differences. This comparison can be done with two different scripts or between the same scripts of different versions.

To compare scripts:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the script that you want to compare.
3. Select **Compare Script Versions** from the Actions menu.

The **Compare Scripts** dialog box appears.

4. Use the **Source script** and **Target script** lists to select the scripts that you want to compare.
5. Use the **Version** lists to specify the versions of the source and target scripts that you have selected.
6. Click **Compare**.

The differences between the scripts are displayed. Use the **Next Diff** and **Prev Diff** buttons to navigate to the next change or the previous change, respectively.

The differences between the two scripts are represented using three different colors:

- Green— The green lines represent the changes that appear only in the source script.
- Blue— The blue lines represent the changes that appear only in the target script.
- Purple— The purple lines represent the changes that are different between the two scripts.

After the **Next Diff** and **Prev Diff** buttons, the total number of differences, the number of differences in the source script, the number of differences in the target script, and the number of changes are displayed.

7. Click **x** to close the window and return to the Scripts page.

Related Documentation

- [Modifying a Script on page 297](#)
- [Staging Scripts on Devices on page 300](#)
- [Scripts Overview on page 275](#)

Deleting Scripts

You can use Junos Space Network Management Platform to delete the scripts that you import into the Junos Space server. When you delete a script, all versions of that script and the checksum verification results associated to that script are deleted.

To delete scripts:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the scripts that you want to delete.



NOTE: Only the scripts that are not associated to any of the device(s) can be deleted. You need to remove scripts from device before deleting it from Junos Space Network Management Platform. When you delete a script, all versions of that script and the checksum verification results associated to that script are deleted.

3. Select **Delete Scripts** from the Actions menu.

You will receive a confirmation message before you delete the script. If you have not removed scripts from device before deleting it from Junos Space Network Management Platform, you will receive an action failure message.

The **Delete Device Scripts** dialog box lists the scripts that you chose for deletion.

4. Click **Confirm**.

The selected scripts are deleted and the **Jobs** dialog box displays a job ID link. You can click the link to view the status of the delete operation on the Jobs page.

5. Click **Cancel** to return to the Scripts page.

Related Documentation

- [Modifying a Script on page 297](#)

Staging Scripts on Devices

Junos Space Network Management Platform enables you to stage a single script or multiple scripts on one device or on multiple devices simultaneously. Staging a script enables you to hold a script on a device, ready to be executed when required. Scripts that are staged list only the devices that are not associated to any of the selected script and to the devices with older versions of the selected scripts. This allows you to associate scripts to new devices and also upgrade scripts to the latest version on already associated devices.

To stage a script on devices:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

2. The **Scripts** page appears.

3. Select the scripts that you want to stage on one or more devices. The selected scripts are highlighted.

4. Select **Stage Scripts on Devices** from the Actions menu.

The **Stage Scripts on Devices** page appears, which displays:

- A list of the selected scripts and the latest version of the script. By default, the latest version of the script is staged on the selected devices. However, to stage a previous version of the script, select the suitable version from the drop-down list below the Version column.
 - A list of the Junos Space Network Management Platform devices that are not associated to any of the selected scripts and also the devices with the older versions of the selected scripts.
5. Keep the **Enable Scripts** check box selected if you want the scripts to be enabled and ready to be executed when you stage them on devices from Junos Space Network Management Platform. Clear this check box if you want the scripts to be disabled on the devices.
 6. (Optional) To view all the devices, select **Show existing Staged Devices**.
 7. Select a device to stage this selected script.

You can select devices by using two selection modes—manual and tag-based. To select devices manually, click the **Select by Device** option. To select devices based on tags, click the **Select by tags** option. These two options are mutually exclusive. If you select one, the other is disabled.

8. (Optional) To schedule a time for staging the device image, select the **Schedule at a later time** check box and use the lists to specify the date and time.
9. Click **Stage**. The script is staged on the selected device or devices. The **Stage Scripts Information** page displays the job ID.
10. To verify the status of this job, click the job ID to view the details, or close the page to go back to the **Scripts** page.

If there is a failure in the staging of the script, you can view the reason for failure within the job description.

11. Click **View** under **Associations** column of that staged script to view the details of the Script - Device association, which includes script name, script type, host name, IP address, platform, software, correct staged script version, latest version, and activation status. If you need to view the associated devices for multiple scripts, see [“Viewing Device Association of Scripts” on page 301](#).

Related Documentation

- [Scripts Overview on page 275](#)
- [Viewing Device Association of Scripts on page 301](#)

Viewing Associated Devices

You can view the details of multiple scripts that got staged to a Junos device or multiple devices using Junos Space Network Management Platform. The script-device association can be viewed from the Scripts landing page by selecting one or more scripts. Clicking on **View** under the **Associations** column displays the associated devices for a single script.

To view the associated scripts:

1. Select **Images and Scripts > Scripts**.

The Scripts page appears.

2. Select a script.



NOTE: Make sure that the script has already got staged to the devices using Junos Space Network Management Platform.

3. Select **View Associated Devices** from the Actions menu.
4. The View Associated Devices page appears with valid Script - Device(s) association details, which includes script name, script type, IP address, platform, software version, correct staged script version, latest script version, and activation status.
5. Click **Return to Script Inventory View** to go back to the **Scripts** page.

- Related Documentation**
- [Scripts Overview on page 275](#)
 - [Staging Scripts on Devices on page 300](#)

Verifying the Checksum of Scripts on Devices

A script that is transferred to a device can be corrupt. Verifying the checksum of the scripts that use Junos Space Network Management Platform ensures that the transferred script is not corrupt. Junos Space Network Management Platform enables you to verify the checksum of multiple scripts that are deployed on the devices.

When you verify scripts that have multiple versions, the latest version of selected scripts are verified with the version of script that is available on the device. If the version of the script present on the device does not match the version that it is compared with, you will be notified by an error message.

To verify the checksum of a script:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the script whose checksum you want to verify.
3. Select **Verify Scripts on Devices**.

The **Verify Checksum of Scripts on Device(s)** dialog box appears.

4. Select the devices that have the script deployed on them, by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

5. To select devices manually:
 - Click the **Select by Device** option and select the device(s) that have the script deployed on them. The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.
 - To select all the devices, select the check box in the column header next to Host Name.
6. To select devices based on tags:
 - Click the **Select by Tags** option. The Select by tags list is activated.
 - Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
 - Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.
7. To schedule a time for verification, select the **Schedule at a later time** check box and use the lists to specify the date and time when you want the script to be verified.
8. Click **Verify Checksum**.

The result of this verification appears, and a **Jobs** dialog box displays a job ID link. You can click the link to view the status of the verification operation on the Jobs page. To display the checksum verification results, see [“Viewing Verification Results” on page 336](#).
9. Click **Cancel** to return to the Scripts page.

Related Documentation • [Enabling Scripts on Devices on page 304](#)

Enabling Scripts on Devices

After you stage scripts on devices, you can use Junos Space Network Management Platform to enable these scripts on one or more devices simultaneously.

When you enable scripts that use Junos Space Network Management Platform, depending on the type of script, an appropriate configuration is added on the device. For example, for a file named `bgp-active.slax`, the configuration added to the device is as follows:

- For a commit script:
Example: [edit]
user@host# set system scripts commit file bgp-active.slax
- For an op script:
Example: [edit]
user@host# set system scripts op file bgp-active.slax
- For an event script:
Example: [edit]
user@host# set system scripts event file bgp-active.slax



CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is enabled regardless of its contents.

To enable scripts on devices:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select one or more scripts that you want to enable on devices.
3. Select **Enable Scripts on Devices** from the Actions menu.

The Enable Scripts on Device(s) page appears.



NOTE:

- This operation does not list the devices that are not associated. It also does not list the devices wherein the script is in already enabled state.
- Only commonly associated devices will be listed for multiple selection.

4. Select the devices on which you want the script to be enabled, by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

5. To select devices manually:
 - Click the **Select by Device** option and select the device(s) on which you want to enable the device script. The Select Devices status bar shows the total number of devices that you have selected, dynamically updating as you select.
 - To select all the devices, select the check box in the column header next to Host Name.
6. To select devices based on tags:
7. Click the **Select by Tags** option. The Select by tags list is activated.
8. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
9. Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.
10. To schedule a time for enabling the script, select the **Schedule at a later time** check box and specify the date and time when you want the script to be enabled.
11. Click **Enable**.

The selected scripts are enabled on the devices, and the **Jobs** dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Jobs page.

Click **Cancel** to return to the Scripts page.

Related Documentation

- [Executing Scripts on Devices on page 309](#)

Disabling Scripts on Devices

After you deploy scripts on devices, you can use Junos Space Network Management Platform to disable these scripts on one or more devices simultaneously.

When you disable scripts that use Junos Space Network Management Platform, the configuration added on the device is similar to the following:

For example, for a file named `bgp-active.slax`, the configuration added is:

```
user@host# delete system scripts commit file bgp-active.slax
```



CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is disabled regardless of its contents.

To disable scripts on devices:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select one or more scripts that you want to disable on devices.
3. Select **Disable Scripts on Devices** from the Actions menu.



NOTE:

- This operation lists only the associated devices by default. Also, the associated devices should have the script in enabled state.
- The already associated devices should have the latest script version, otherwise those devices are also not displayed for the device selection

The Disable Scripts on Device(s) page appears.

4. Select the devices on which you want the script to be disabled, by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

5. To select devices manually:
 - Click the **Select by Device** option and select the device(s) that have the script deployed on them. The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.
 - To select all the devices, select the check box in the column header next to Host Name.

6. To select devices based on tags:
 - Click the **Select by Tags** option. The Select by tags list is activated.
 - Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
 - Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.
7. To schedule a time for disabling the script, select the **Schedule at a later time** check box and specify the date and time when you want the script to be disabled.
8. Click **Disable**.
 The selected scripts are disabled on the devices, and the **Jobs** dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Jobs page.

Click **Cancel** to return to the Scripts page.

Related Documentation

- [Scripts Overview on page 275](#)

Removing Scripts from Devices

You can use Junos Space Network Management Platform to remove the scripts from the devices. The **Remove Script from Devices** option lists only the devices that are currently associated to the selected script(s). For multiple selection, only the commonly associated devices are listed.



CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is removed regardless of its contents.

To remove scripts from devices:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the script that you want to remove from the device.
3. Right-click your selection or use the Actions menu, and select **Remove Scripts from Devices**.

The **Remove Scripts from Device(s)** page appears.

The **Remove Scripts from Device(s)** dialog box lists the devices the script is associated with.

4. Select the devices from which you want the script to be removed, by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled..



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed. For multiple selection, only commonly associated devices are listed.

5. To select devices manually:
 - Click the **Select by Device** option and select the device(s) that have the script deployed on them. The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.
 - To select all the devices, select the check box in the column header next to Host Name.
6. To select devices based on tags:
 - Click the **Select by Tags** option. The Select by tags list is activated.
 - Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
 - Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.

- The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
- Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.



NOTE: The **Force Remove** check box provides an option to remove the script-device association from Junos Space Network Management Platform even if it is unable to remove the script(s) from the device(s) due to any connectivity issues. This option needs to be turned on while removing the scripts. The script - device association will be removed regardless of whether this operation has failed or not.

7. Click **Remove**.

The script is removed from the selected devices, and a **Jobs** dialog box displays a job ID link. You can click the link to view the status of the script removal operation on the Manage Jobs page.

8. In the **Manage Scripts** page, click **View** listed under the **Associations** column of those scripts, one by one. The **View Associated Devices** page is displayed with the script - device association details removed for those scripts that got removed.

Click **Cancel** to return to the Scripts page.

**Related
Documentation**

- [Staging Scripts on Devices on page 300](#)
- [Scripts Overview on page 275](#)

Executing Scripts on Devices

You can use Junos Space Network Management Platform to trigger the execution of op scripts on one or more devices simultaneously. Commit and event scripts are automatically activated after they are enabled. Commit scripts get triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or if a time is specified.



CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is executed regardless of its contents.

To execute an op-script on devices:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Select the op-script that you want to execute on a device.
3. Select **Execute Script on Device(s)** from the Actions menu. This option is enabled only when the script is staged and is in the enabled state.

The Execute Script on Device(s) page appears.

By default, this page lists the devices on which the latest version of the script is staged. If no devices are listed, it means that the latest version of the script is not staged yet. If you have staged the previous versions of the script, select one of the staged versions from the Version list. The page displays the list of devices on which this version of the script is staged. A quick way to find out which version of the script is staged, click **View** under **Associations** from the Scripts page. The **Staged Version** column provides you with this information.

4. Select the devices on which you want the script to be executed, , by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

5. To select devices manually:
 - Click the **Select by Device** option and select the device(s) that have the script deployed on them. The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.
 - To select all the devices, select the check box in the column header next to Host Name.
6. To select devices based on tags:
 - Click the **Select by Tags** option. The Select by tags list is activated.
 - Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears.
 - The list displays two subcategories of tags—Public and Private.
 - A check box is available next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - When you enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.

- Select the check boxes next to the displayed tag names as desired, or search for specific tags. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the selected devices and their details.
7. To specify the parameters for script execution, click **Add Parameters**, and specify the parameter name and value in the row that appears.
 8. To schedule a time to execute the script, select the **Schedule at a later time** check box and specify the date and time when you want the script to be executed.
 9. Click **Execute**.

The selected scripts are executed on the devices, and the Jobs dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page. Double click the task to view the Script Management Job status window. Click the View Results link under Description column to view the results of Script Execution. The result HTML is processed and rendered to allow you to read and understand the Script Execution Results.

Click **Cancel** to return to the Scripts page.

You can view the script execution from the Manage Devices page by selecting one or more devices and selecting View Script Executions from the right click context menu. The script execution result of the script can also be viewed from Manage Scripts page by clicking the View link in the Results column of the View Executions Results window. This option displays only the results of any OP scripts executed on the device and not the Commit or Event scripts.

**Related
Documentation**

- [Enabling Scripts on Devices on page 304](#)
- [Executing Scripts on Devices Remotely with JUISE on page 104](#)

Viewing Execution Results

You can use Junos Space Network Management Platform to trigger the execution of op script on one or more devices simultaneously. You can also view the execution result of the script.

To view the execution results:

1. Select **Images and Scripts > Scripts**.

The **Scripts** page appears. From the tool bar on the top right corner of the page, click the icon to open the **View Execution Results** page.

The **View Execution Results** page appears. This page displays the execution history that includes script version, host name, script name, execution status, job result, execution start time and end time.

The fields Host Name, Script Name, Version, and Status have the drop down list enabled with the filter option, which has an input field wherein you can enter the filter criteria. If you apply the filters, the table contents display only the values that match the filter criteria. The fields Results, Execution Start Time and Execution End Time do not support the filter option.

[Table 52 on page 312](#) describes the information that appears on the View Execution Result page.

Table 52: View Execution Result Page Fields Description

Field	Description
Host Name	Name of the Device in which the script is executed
Script Name	Name of the script
Version	Executed version of script
Status	Script Execution Job status
Results	Contains a link to view the Script Execution Results
Execution Start Time	The time at which the Execution started
Execution End Time	The time at which the Execution ended

- Click **View** under the **Results** column to view the detailed execution results.

The Execution Result details dialog box displays the script name, version, Host name, Results, Execution Start time and Execution End time. The results displayed in the Execution Result Details page are in the raw HTML format.

- To view only the result of script Execution click **View** in the Results column.

The Script Execution Job Results page is displayed with the following details like- Device name, Entity name, Script Execution status and Script Execution Result. The result HTML is processed and rendered to allow you to read and understand the Script Execution Results.

Related Documentation

- [Scripts Overview on page 275](#)

Importing Scripts

Using Junos Space Network Management Platform, you can import a single script or multiple scripts (the maximum is 680) at a time to the Junos Space server by clicking the **Add Device Scripts** button. To import scripts, you must first save the scripts on the local file system of your workstation or client, ensure that they are of .slax or .xsl format, and also ensure that they are commit, operation (op), or event scripts.

After importing scripts, you can perform the following tasks:

- View script contents
- Export scripts
- Modify scripts
- Compare scripts
- Verify the checksum of scripts
- View verification results
- Enable and disable scripts on devices
- Remove scripts from devices
- Execute scripts on devices
- Deploy scripts on one or more devices simultaneously

Prior to Junos 9.0, event scripts and op scripts were saved in op directory and enabled under system scripts op hierarchy. However, beginning in Junos 9.0, event scripts are saved in event directory, and enabled under event-script hierarchy.



NOTE: If you want to import multiple scripts at a time, use the **Firefox** or **Chrome** Web browser. Currently, **Internet Explorer** does not support selection of multiple files. In addition, note that two scripts with the same name cannot be imported into Junos Space server.

To import scripts to Junos Space Network Management Platform:

1. From the task bar, select **Network Management Platform > Images and Scripts > Scripts > Import Script**.

The Import Script box appears.

2. Click the **Add Device Scripts** button . The Add Device Scripts window appears.
3. Click **Browse**. The file upload dialog box displays the directories and folders on your local file system.
4. Select the script or scripts that you want to import (you can select a maximum of 680 scripts at a time), and click **Open**.

5. Click **Add Script** to upload the scripts, or click **Cancel** if you want to go back to the **Import Script** box.



NOTE: When you upload multiple scripts, the files are saved on the Junos Space server in the temporary directory `/var/cache/jboss/Script_temp`, where temporary session folders are created and deleted. If you do not log out of Junos Space system using the **Log Out** button, the temporary session folders are deleted after 30 mins.

If the selected scripts are valid, they are displayed on the **Import Script** page. If the selected scripts are invalid, you get a failure notice.

A script might be valid but of an unrecognized type. That is, it has the correct extension (.xls or .slax) but does not use the correct boilerplate. If you attempt to upload a script that Junos Space Network Management Platform does not recognize, you get a script error. You can choose to either import or discard the unrecognized script.

6. If you want to remove any script(s) that are displayed in the **Import Script** box, select the script(s) and click the **Delete Scripts** button.
7. Click **Import Scripts**. The selected scripts are uploaded into Junos Space Network Management Platform and displayed on the **Scripts** page.
8. Click **Cancel** to return to the **Scripts** page.

Related Documentation

- [Viewing Script Details on page 335](#)

Configuration: Operations

- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Deleting an Operation on page 320](#)
- [Exporting an Operation in TAR Format on page 320](#)
- [Importing an Operation on page 322](#)

Creating an Operation

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS. Junos Space Network Management Platform allows you to create operations that combine multiple scripts and image tasks, such as deploying images and deploying or executing scripts, into a single operation for efficient use and reuse.

An operation can contain any number of scripts and other existing operations, but only one device image at a time.

To create an operation:

1. Select **Network Management Platform > Images and Scripts > Operations** and click the Create Operation icon.

The Create Operation page appears.

2. Enter a name and description for the operation.
3. Click the Add (+) icon, and select **Script**, **Image**, or **Operation** from the list.

The **Select Scripts**, **Select Images**, or **Select Operations** dialog box appears depending on what you selected and displays all the Junos Space Network Management Platform scripts, images, and operations, respectively, that you can include in the operation.

- To add a script, click the Add (+) icon, and select **Script** from the list. The **Select Scripts** dialog box appears.

Select the scripts and click **Add** to add your selections to the list.

Click the Edit icon next to the script to modify:

- The action that the script should perform: **Stage** (default) or **Execute**.
- The version of the script to be associated with the operation. By default, the latest version is selected. To change the version, select the suitable version of the script from the **Version** list (preferably the version that you have staged; else, Junos Space Network Management Platform throws an error when you run the operation).
- Keep the **Enable Scripts** check box selected if you want the scripts to be enabled and ready to be executed when you stage them from Junos Space Network Management Platform. Clear this check box if you want the scripts to be disabled on the devices. However, before you run the operation make sure that the scripts are enabled; else, Junos Space Network Management Platform throws an error.
- Script return code—Junos Space, by default, returns “Success” when it is able to execute a script successfully. However, you may want to consider the script execution to be a success or a failure only if a specific pattern string is present in the script execution results. You can specify this pattern string in the “Set value” field. This field supports up to a maximum of 255 characters.

For example, consider you are running a script to verify whether all the interfaces on a device are up. Though the script might execute successfully, you may want to show this script execution as a failure if an interface is down. To achieve this, you can search for the string “down” in the script execution results using the following steps:

- a. Select **Failure**.
- b. In the **Set value** field, type **down**.

Click **Save** to save the configuration changes to the script.

- To add an image, click the Add (+) icon, and select **Image** from the list. The **Select Images** dialog box appears.

Select the images and click **Add** to add your selections to the list.

You can also edit the action that image should perform (**Stage** or **Deploy**), and various other deployment options. See [“Deploying Device Images” on page 286](#) for more information.

- To add an operation, click the Add (+) icon, and select **Operation** from the list. The **Select Operation** dialog box appears.







Select the operations and click **Add** to add your selections to the list.



NOTE: You cannot edit a child operation.

4. You can modify the list of selected scripts, images, and operations using the icons described in [Table 53 on page 317](#).

Table 53: Create Operation Dialog Box Icon Descriptions

Icon	Description
	Add scripts, image, and operations to the list.
	Delete the selected script, image, or operation from the list.
	Move the selected script, image, or operation to the row above.
	Move the selected script, image, or operation to the row below.
	Make a copy of the selected script, image, or operation, and include it in the operation.
	Edit the options for deploying or executing the scripts or images in the operation. For scripts, you can edit the action type, script parameters, and their values (success or failure). For images, you edit the image deployment options. See “Deploying Device Images” on page 286 for more information. NOTE: You cannot edit a child operation

- Click **Create** to create the operation and go the Operations page.

To verify whether the operation is created with your specifications, double-click the operation and view its details.

Related Documentation

- [Operations Overview on page 279](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)
- [Deleting an Operation on page 320](#)
- [Exporting an Operation in .tar Format on page 320](#)
- [Importing an Operation on page 322](#)

Modifying an Operation

Junos Space Network Management Platform allows you to edit the parameters of an operation.

To modify an operation:

1. Select **Images and Scripts > Operations**.

The Operations page displays all the operations in the Junos Space Network Management Platform database.

2. Select the operation that you want to modify.
3. Click the **Modify Operation** icon.
4. Modify the necessary parameters. See [“Creating an Operation” on page 315](#) for more information.
5. Click **Modify** to save your changes and go to the Operations page.

To verify whether your changes are saved, double-click the operation and view its details.

Related Documentation

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)
- [Deleting an Operation on page 320](#)
- [Exporting an Operation in .tar Format on page 320](#)
- [Importing an Operation on page 322](#)

Running an Operation

Junos Space Network Management Platform allows you to execute (or run) operations existing in the Junos Space Network Management Platform database on devices.

To run an operation:

1. Select **Network Management Platform > Images and Scripts > Operations**.

The Operations page displays all the operations in the Junos Space Network Management Platform database.

2. Select the operation that you want to execute.
3. Select **Run Operation** from the Actions menu.

The Run Operation page appears.

4. Select the devices on which you want to execute the operation.

You can search for specific devices by entering the name of the device in the Find Devices search box.

5. You can also specify a tag for the selected devices so that you can reuse the same group of devices to run a different operation.
6. Click **OK** to run your operation immediately.

You can also schedule a time for the operation to run by selecting the **Schedule at a later time** check box, specifying the date and time when you want to run the operation, and then clicking **Execute**.

The selected operation is executed on the devices, and the Jobs dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Jobs page. The results are displayed in an easy-to-read format and does not contain any < output > tags.

Related Documentation

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)
- [Deleting an Operation on page 320](#)
- [Exporting an Operation in .tar Format on page 320](#)
- [Importing an Operation on page 322](#)

Copying an Operation

You can use Junos Space Network Management Platform to create copies of operations existing in the Junos Space Network Management Platform database.

To create a copy of an operation:

1. Select **Network Management Platform > Images and Scripts > Operations**.

The **Operations** page displays the operations in Junos Space Network Management Platform.

2. Select the operations that you want to copy.
3. Select **Copy Operation** from the Actions menu.

The **Copy Operation** dialog box appears, prompting you to enter a new name for the operation.

4. Enter a new name for the operation in the **Destination Name** box.
5. Click **Copy** to create a copy of the operation and go back to the Operations page.

Related Documentation

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)

- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Deleting an Operation on page 320](#)
- [Viewing Operations Results on page 339](#)

Deleting an Operation

You can use Junos Space Network Management Platform to delete operations from the Junos Space Network Management Platform database.

To delete an operation:

1. From the taskbar, select **Network Management Platform > Images and Scripts > Operations**.

The Operations page displays the operations in Junos Space Network Management Platform.

2. Select the operations that you want to delete.
3. Select **Delete Operations** from the Actions menu.

The **Delete Operations** dialog box lists the operations that you chose for deletion.

4. Click **Confirm** to delete the operation.

The selected operations are deleted and the **Jobs** dialog box displays a job ID link. You can click the link to view the status of the delete operation on the Jobs page.



NOTE: When you delete an operation, you do not delete the scripts, images or operations associated with it.

Related Documentation

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)

Exporting an Operation in TAR Format

You can use Junos Space Network Management Platform to export operations from the Junos Space Network Management Platform database to your local file system. The export operation does not delete the operations that you export from the Junos Space Network Management Platform database. It enables you to have a local copy of the

operations, which you can transfer among multiple Junos Space Network Management Platform instances for efficient use and reuse. It also allows you to make any configuration changes to the operations, locally (offline).

The operations are exported in tar format. The exported file does not include any objects that are referenced within the operations. For example, if an operation includes an action on an image or a script, exporting the operation does not export the referenced image or script.

To export an operation:

1. Select **Images and Scripts > Operations**.

The Operations page appears.

2. Select operations on this page.
3. Select **Export Operations** from the Actions menu.

The Export Operations page appears indicating that the selected operations are exported in tar format.

If you have not selected any operations, then Export Operations is disabled. Select operations to enable this option.

4. Click **OK**.

The File Open dialog box enables you to save the operation files in the tar format and the **Export Operations Job Status** dialog box displays the status of this task. To view the status of your job in the Job Manager, click the bar on this dialog box. You can also save the tar file by clicking the Download link.

5. Click **OK** and save the files on your local file system.
6. Unzip the file to view the contents.



NOTE: When you export a nested operation (that is, an operation containing one or more operations), each operation is exported as a separate XML file. For example, when you export a nested operation A containing operation B and operation C, the extracted folder contains three XML files, one for each operation.

Related Documentation

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)
- [Deleting an Operation on page 320](#)

- [Importing an Operation on page 322](#)

Importing an Operation

You can use Junos Space Network Management Platform to import operations to the Junos Space Network Management Platform database from your local file system. The operation that you import should be an XML file (for example, operation-test.xml). Before you import operations, make sure that:

- They are of .xml format
- The objects that are referenced in the operations exist in the Junos Space Network Management Platform instance to which you are importing. Else, Junos Space Network Management Platform throws an error and the operation is not imported.

To view the syntax of an operation XML file, you can create and download an operation from Junos Space Network Management Platform to your local file system (through the export operation) and open the XML file in an XML editor.



NOTE: If you want to import multiple operations at a time, use the Firefox or Chrome Web browser. Currently, Internet Explorer does not support selection of multiple files. In addition, note that two operations with the same name cannot be imported into the Junos Space server.

To import operations to Junos Space Network Management Platform:

1. Select **Images and Scripts > Operations**.

The Images and Scripts > Operations page appears.

2. Select the **Import Operation** icon.

The Import Operations page appears.

3. Click the **Add Operations (+)** icon.

The Add Operations page appears.

4. Click **Browse** and select the operations from your local file system.



NOTE: Use Firefox or Chrome to import multiple operations. Currently, using IE, you can import only single file at a time.

5. Click **Add Operations**.

If the selected operations are valid, they are displayed on the Import Operations page.
If the selected operations are invalid, you get a failure notice.

6. Click **Import Operation**.

If the operation of the same name exists in Junos Space Network Management Platform, you are asked whether you want to overwrite the existing operation. Click **Yes** to overwrite; else, click **No**.

7. If the operations are imported successfully, Junos Space Network Management Platform displays a success message. Click **OK** on this message.

However, if the imported operation references an object (script, image, or operation) that is not present in the target Junos Space Network Management Platform instance, Junos Space Network Management Platform throws an error message and the operation is not imported.

Sample error message:

No operation file(s) are imported. Referenced operation test-operation-1 in Operation test-operation-nested does not exist!

**Related
Documentation**

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Viewing Operations Results on page 339](#)
- [Deleting an Operation on page 320](#)
- [Exporting an Operation in .tar Format on page 320](#)

Configuration: Script Bundles

- [Creating a Script Bundle on page 325](#)
- [Modifying a Script Bundle on page 326](#)
- [Deleting Script Bundles on page 327](#)
- [Staging Script Bundles on Devices on page 328](#)
- [Executing Script Bundles on Devices on page 329](#)
- [Enabling Scripts in Script Bundles on Devices on page 330](#)
- [Disabling Scripts in Script Bundles on Devices on page 332](#)

Creating a Script Bundle

Junos Space Network Management Platform allows you to group multiple op and commit scripts into a script bundle. To create a script bundle, you must first import the scripts that you want to include in the script bundle, into Junos Space Network Management Platform (see [“Importing Scripts” on page 313](#)).

To create a script bundle:

1. Select **Network Management Platform > Images and Scripts > Script bundles** and select the Create Script Bundle icon.

The Create Script Bundle page appears.

2. Enter a name and description for the script bundle.
3. Click the Add Scripts (+) icon to add scripts that need to be included into the script bundle.

The Select Scripts page displays all Junos Space Network Management Platform scripts that you can include into the script bundle.

4. Select the scripts that you want to include in the script bundle.
The selected scripts are highlighted.

5. Click **Add**.







The selected scripts are included in the **Selected Scripts** section of the **Create Script Bundle** dialog box.

You can edit the script parameters, rule, and version from the Selected Script section. By default, the latest version of the script is associated with the script bundle. To

change the version of the script, click the Edit icon next to **selected Version** for the script and select the suitable version. After selection, click **Save**.

You can modify the list of selected scripts using the icons described in [Table 54 on page 326](#).

Table 54: Create Script Bundle Dialog Box Icon Descriptions

Icon	Description
	Add scripts to the script bundle.
	Delete the selected script from the script bundle.
	Move the selected script to the row above.
	Move the selected script to the row below.
	Make a copy of the selected script and include it in the script bundle.
	Edit the value (success or failure) of script parameters. This option is disabled when commit scripts are selected.

- Click **Save**.
The script bundle is created and displayed on the Script Bundles page.
- To verify whether the script bundle is created with your specifications, double-click the script bundle and view its details.

Related Documentation

- [Staging Script Bundles on Devices on page 328](#)
- [Modifying a Script Bundle on page 326](#)
- [Scripts Overview on page 275](#)

Modifying a Script Bundle

Junos Space Network Management Platform allows you to modify a script bundle name, description, number of scripts included in the script bundle, and script parameter value (success or failure) of every script included in the script bundle.

To modify script bundles:







- Select **Images and Scripts > Script bundles**.

The Script Bundles page displays all Junos Space Network Management Platform script bundles.

- Select the script bundle that you want to modify.

- 3. Select **Modify** from the Actions menu.
The **Modify Script Bundle** dialog box appears.
- 4. Make your changes to the script name, script parameters, value (success or failure) of every script included in the script bundle, the version of the script to be associated with the script bundle, or the description of the script bundle. You can modify the list of selected scripts using the icons described in [Table 55 on page 327](#).

Table 55: Modify Script Bundle Dialog Box Icon Descriptions

Icon	Description
	Add scripts that are not included in the script bundle.
	Delete the selected script from the script bundle.
	Move the selected script to the row above.
	Move the selected script to the row below.
	Make a copy of the selected script and include it in the script bundle.
	Edit the value (success or failure) of script parameters or script version. This option is disabled when commit scripts are selected.

- 5. Click **Modify**.
Your modifications are saved and the Script Bundles page appears.
- 6. To verify whether your changes are saved, double-click the script bundle and view its details.

- Related Documentation
- [Staging Script Bundles on Devices on page 328](#)
 - [Executing Script Bundles on Devices on page 329](#)
 - [Scripts Overview on page 275](#)

Deleting Script Bundles

Junos Space Network Management Platform enables you to delete multiple script bundles.

To delete script bundles:

1. From the taskbar, select **Images and Scripts > Script bundles**.

The Script Bundles page displays all Junos Space Network Management Platform script bundles.

2. Select the script bundles that you want to delete.

3. Select the **Delete Script Bundles** icon.

The **Delete Device Script Bundles** dialog box displays the names of the selected script bundles.

4. Click **Delete** to confirm.

The selected script bundles are deleted and the Script Bundles page appears.

5. To verify whether the script bundles are deleted, view the list of scripts in the Script Bundles page.

Related Documentation

- [Creating a Script Bundle on page 325](#)
- [Executing Script Bundles on Devices on page 329](#)
- [Scripts Overview on page 275](#)

Staging Script Bundles on Devices

Junos Space Network Management Platform allows you to stage script bundles on devices. During script bundle deployment, op scripts and commit scripts are copied to the /var/db/scripts/op directory on the device. When you stage script bundles on dual Routing Engines, the script bundles are copied to both Routing Engines, and in case of Virtual Chassis, the script bundles are copied to all of the FPCs.

To stage script bundles on devices:

1. Select **Network Management Platform > Images and Scripts > Script bundles**.

The Script Bundles page displays all Junos Space Network Management Platform script bundles.

2. Select the script bundles that you want to deploy on devices.

3. Select the script bundles that you want to stage on devices.

4. Select **Stage on Devices** from the Actions menu.

The **Stage Script Bundle On Device(s)** dialog box appears.

5. Keep the **Enable Scripts** check box selected if you want the scripts to be enabled and ready to be executed when you stage them from Junos Space Network Management Platform.

If you want the scripts to be disabled while staging them on the devices, clear this check box. However, before you run the script bundle make sure that the scripts are enabled; else, Junos Space Network Management Platform throws an error.

6. Select the **Show existing Staged Devices** check box to display the devices in which the scripts are staged. When this check box is selected, the **Select Devices** section displays the devices in which the scripts are staged along with the devices in which the scripts are not staged.
7. Select the devices on which you want to stage the script bundles.
8. To schedule a time for deploying the script bundles, select the **Schedule a later time** check box and specify the date and time when you want the script bundles to be deployed.
9. Click **Stage**.
The selected scripts are deployed and a **Jobs** dialog box displays a job id link, which you can click to view the status of the script bundle deployment.
10. Click **OK**.
The script bundles are deployed on the selected devices and the Script Bundles page appears.

Related Documentation

- [Creating a Script Bundle on page 325](#)
- [Modifying a Script Bundle on page 326](#)
- [Deleting Script Bundles on page 327](#)
- [Executing Script Bundles on Devices on page 329](#)
- [Enabling Scripts in Script Bundles on Devices on page 330](#)
- [Disabling Scripts in Script Bundles on Devices on page 332](#)
- [Script Bundles Overview on page 281](#)

Executing Script Bundles on Devices

Junos Space Network Management Platform allows you to execute script bundles on devices. When you execute script bundles, Junos Space Network Management Platform triggers the execution of op scripts on the selected devices. Commit scripts are executed on commit when events occur on the device and therefore the result of the script bundle execution for commit scripts is always shown as Success in Junos Space Network Management Platform.

To execute script bundles on devices:

1. Select **Network Management Platform > Images and Scripts > Script bundles**.
The Script Bundles page displays all Junos Space Network Management Platform script bundles.
2. Select the script bundles that you want to execute on devices.
3. Right-click your selection or use the Actions menu, and select **Execute on Devices**.
The **Execute Script Bundle On Device(s)** dialog box appears.

To redeploy the scripts before execution, keep the **Stage & Enable Scripts before Execution** check box selected (the default). If the scripts within the script bundle are

previously staged and enabled in all the necessary devices and you do not want to redeploy these scripts, clear this check box.

4. Select the devices on which you want to execute the scripts.
5. You can modify the script parameters before executing script bundles on devices. The changes made to script parameters are saved only on the devices on which the script bundle is executed. The script parameters in the script bundle in Junos Space Network Management Platform continues to reflect the original values.

To edit the script parameter values before execution:

1. Click the **Update Script Parameters/Rule** link. The **Configure Script Bundle Parameters** dialog box appears.
2. Use the Edit icon to set the script parameter value to Success or Failure, and click **Save**.
3. Click **Configure**. Your changes are saved and the **Enable Script Bundle On Device(s)** dialog box displays your previous selections.
6. To schedule a time for deploying the script bundles, select the **Schedule a later time** check box and specify the date and time when you want the script bundles to be executed.
7. Click **Execute**.
The script bundle is enabled on the selected devices and a **Jobs** dialog box displays a job id link, which you can click to view the status of script bundle execution.
8. Click **OK**.

The selected script bundle is executed on the devices and the Jobs dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Jobs page. The results are displayed in an easy-to-read format and does not contain any < output > tags.

Related Documentation

- [Creating a Script Bundle on page 325](#)
- [Modifying a Script Bundle on page 326](#)
- [Deleting Script Bundles on page 327](#)
- [Staging Script Bundles on Devices on page 328](#)
- [Enabling Scripts in Script Bundles on Devices on page 330](#)
- [Disabling Scripts in Script Bundles on Devices on page 332](#)
- [Script Bundles Overview on page 281](#)

Enabling Scripts in Script Bundles on Devices

After you stage the script bundle, you can use Junos Space Network Management Platform to enable the scripts within the script bundle on one or more devices simultaneously.

To enable the scripts on devices:

1. Select **Images and Scripts > Script bundles**.

The Script Bundles page appears, which displays all Junos Space Network Management Platform script bundles.

2. Select the script bundle containing the scripts that you want to enable on devices.
3. Select **Enable Script Bundle on Devices** from the Actions menu. If this option is disabled, it means that one or more of the scripts within the script bundle are not staged on any of the devices. You may want to stage the scripts first and then proceed to enable the scripts.

The Enable Script Bundle On Device(s) page appears. However, if all the scripts within the script bundle are enabled on all the associated devices, then Junos Space Network Management Platform displays the following message indicating that there are no scripts that can be enabled.

No devices found where all the scripts of the selected bundle are staged and at least one script is disabled



NOTE: The following devices are listed on the Enable Script Bundle On Device(s) page:

- Devices on which the scripts within the script bundle are associated
- Devices on which scripts are in the enabled state. If a script is disabled on a device, then that device is not listed.
- Devices on which the version of a script within the script bundle matches the version of the script staged on the devices. If there is a mismatch on the versions of the script, then that device is not listed.

4. Select the devices on which you want the script to be enabled.
5. Click **Enable**.

The scripts within the script bundle are enabled on the selected devices and an Enable Script Bundle Information dialog box displays a job id link, which you can click to view the status.

6. Click **OK**.

Related Documentation

- [Disabling Scripts in Script Bundles on Devices on page 332](#)
- [Creating a Script Bundle on page 325](#)
- [Modifying a Script Bundle on page 326](#)
- [Deleting Script Bundles on page 327](#)
- [Staging Script Bundles on Devices on page 328](#)
- [Executing Script Bundles on Devices on page 329](#)
- [Script Bundles Overview on page 281](#)

Disabling Scripts in Script Bundles on Devices

After you stage the script bundle, you can use Junos Space Network Management Platform to disable the scripts within the script bundle on one or more devices simultaneously.

To disable the scripts on devices:

1. Select **Images and Scripts > Script bundles**.

The Script Bundles page appears, which displays all Junos Space Network Management Platform script bundles.

2. Select the script bundle containing the scripts that you want to disable on devices.
3. Select **Disable Script Bundle on Devices** from the Actions menu. If this option is disabled, it means that one or more of the scripts within the script bundle are not staged on a device.

The Disable Script Bundle On Device(s) page appears, which displays the devices in which the scripts are staged and enabled. However, if all the scripts within the script bundle are disabled, then Junos Space Network Management Platform displays the following message indicating that there are no scripts that can be disabled.

No devices found where all the scripts of the selected bundle are staged and at least one script is enabled



NOTE:

The Disable Script Bundle On Device(s) page lists devices, if a device-script association exists for all scripts in the script bundle with a matching script version. The scripts might be in an enabled or disabled state.

This page does not list devices:

- If the script version in the script bundle does not match the staged version of the script on the devices.
- If all the scripts in the script bundle are in a disabled state on the devices
- If a device-script association does not exist on the device for at least one script (in an enabled or disabled state) in the script bundle.

4. Select the devices on which you want the scripts to be disabled.
5. Click **Disable**.

The scripts within the script bundle are disabled on the selected devices and a Jobs dialog box displays a job id link, which you can click to view the status.

6. Click **OK**.

Related Documentation

- [Enabling Scripts in Script Bundles on Devices on page 330](#)
- [Viewing Device Associations of Scripts in Script Bundles on page 341](#)
- [Modifying a Script Bundle on page 326](#)

- [Deleting Script Bundles on page 327](#)
- [Staging Script Bundles on Devices on page 328](#)
- [Executing Script Bundles on Devices on page 329](#)
- [Script Bundles Overview on page 281](#)

Administration: Scripts

- [Viewing Script Details on page 335](#)
- [Viewing Verification Results on page 336](#)
- [Exporting Scripts in Tar Format on page 337](#)

Viewing Script Details

Using Junos Space Network Management Platform, you can view detailed information about a script, such as its name, type, format, creation time, version, comments, and the contents of the script.

To view the details of a script:

1. Select **Network Management Platform > Images and Scripts > Scripts**.

The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.

2. Double click the script whose details you want to view.

The **Script Details** window displays the script name, type, format, creation time, version, script contents and comments.

[Table 56 on page 335](#) describes the fields displayed in the Script Details page.

Table 56: Script Details Dialog Box Fields

Field	Description
Name	Name of the script file.
Type	Type of script. The values are: <ul style="list-style-type: none">• Commit script• Op script• Event script
Format	Format of the script file. The values are: <ul style="list-style-type: none">• XSL• SLAX

Table 56: Script Details Dialog Box Fields (*continued*)

Field	Description
Creation Time	Date and time when the script was created.
Version	The version number of the script. When you modify a script, the changes are saved in the latest version of the script.
Script Contents	The contents of the script.
Comments	Text that describes the script that is entered by the user.

- Related Documentation**
- [Scripts Overview on page 275](#)
 - [Exporting Scripts in .tar Format on page 337](#)

Viewing Verification Results

You can use Junos Space Network Management Platform to view the results of the checksum verification task. When a verification failure occurs, the results indicate the reason for failure. When you delete a script, the checksum verification results associated to that scrip are also deleted.

To view the verification results:

1. Select **Network Management Platform > Images and Scripts > Scripts**.
The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.
2. Select the script whose verification result you want to view.
3. Right-click your selection or use the Actions menu, and select **View Verification Results**.

The **Script Verification Results** page displays the results of the checksum verification.

[Table 57 on page 336](#) describes the fields on the Script Verification Results page.

Table 57: Script Verification Results Page Fields

Field Name	Description
Script name	Filename of the script that is selected for verifying the checksum.
Device name	Name of the device on which the script is verified.
Result	Result of the verification. The values are: <ul style="list-style-type: none"> • Success • Failed
Start Time	Time when the verification was initiated.

Table 57: Script Verification Results Page Fields (*continued*)

Field Name	Description
Last Update Time	Latest time when the verification was updated.
Remarks	Errors encountered during the verification. This field is blank when the verification is successful.

- Click the **Return to Scripts** link to return to the Scripts page.

Related Documentation

- [Executing Scripts on Devices on page 309](#)

Exporting Scripts in Tar Format

You can use Junos Space Network Management Platform to export the contents of multiple scripts and save them on your local file system.

To export the contents of scripts:

- Select **Images and Scripts > Scripts**.
The Scripts page displays the scripts that you imported into Junos Space Network Management Platform.
- Select the scripts that you want to export.
- Select **Export Scripts** from the Actions menu.
The **Export Scripts** dialog box asks you for a confirmation.
- Click **Export**.
The **File Open** dialog box enables you to save the script files in the tar format and the **Export Scripts Job Status** dialog box displays the status of this task graphically. To view the status of your job in the Job Manager, click the bar of the graph. You can also save the tar files by clicking the **Download** link.
- Click **OK** and save the files on your local file system.
- Unzip the files to view the contents of the script.

Related Documentation

- [Scripts Overview on page 275](#)

Administration: Operations

- [Viewing Operations Results on page 339](#)

Viewing Operations Results

Using Junos Space Network Management Platform, you can view information about operations in the following stages of execution:

- Operations that were successfully executed
- Operations that were not successfully executed
- Operations that are currently being executed
- Operations that are scheduled to be executed later

To view information about an operation:

1. Select **Images and Scripts** > **Operations** and select the View Operation Results icon.

The View Operation Results page appears). The information appears according to the following parameters:

- Operation name
- Date of execution
- Summary of the result (such as the number of devices on which the operation was successfully executed)
- Execution status (scheduled, in progress, success, or failed)
- Job ID

All the parameters in the View Operation Results page have the drop down list enabled with the filter option, which has an input field wherein you can enter the filter criteria. On applying the filter(s), the table contents display only the values that match the filter criteria.

2. Double-click an operation to open the **Operation Result Detail** dialog box, which displays information about the selected operation according to device name and result (success or failed), along with a summary of the operation. Child operations are automatically expanded in the Operation Result Detail of a device. The detail is a flattened list of script or image entries.

You can expand an individual row to view more information about the scripts, images, and child operations (operations within an operation) associated with that device. You can also expand the rows of child operations to see information about all the scripts and images associated with the operation. This way, you are able to monitor the status of each script or image associated with an operation and identify the causes of failed executions (if any).

3. Click **Close** to go back to the View Operation Results page.

**Related
Documentation**

- [Operations Overview on page 279](#)
- [Creating an Operation on page 315](#)
- [Modifying an Operation on page 317](#)
- [Running an Operation on page 318](#)
- [Copying an Operation on page 319](#)
- [Deleting an Operation on page 320](#)

CHAPTER 35

Administration: Script Bundles

- [Viewing Device Association of the Scripts in Script Bundles on page 341](#)

Viewing Device Association of the Scripts in Script Bundles

You can view the devices on which the scripts from the script bundle are staged from Junos Space Network Management Platform.

To view the scripts and their associated devices:

1. Select **Images and Scripts > Script bundles**.

The Script Bundles page displays all Junos Space Network Management Platform script bundles.

2. Select the script bundles.
3. Select **View Associated Devices** from the Actions menu.

Junos Space Network Management Platform displays the scripts (Script Name column) and the devices (Host Name and IP Address columns) to which they are associated along with other details, such as the latest version of the script, script type, staged version of the script, platform of the device, software version running on the device, activation status of the script, and the script bundle to which they belong to.

4. Click **Return to Script Bundle Inventory View** to go back to the Script Bundles page.

Related Documentation

- [Enabling Scripts in Script Bundles on Devices on page 330](#)
- [Disabling Scripts in Script Bundles on Devices on page 332](#)
- [Modifying a Script Bundle on page 326](#)
- [Deleting Script Bundles on page 327](#)
- [Staging Script Bundles on Devices on page 328](#)
- [Executing Script Bundles on Devices on page 329](#)
- [Script Bundles Overview on page 281](#)

CHAPTER 36

Annotations and Examples

- [Scripts Annotations on page 343](#)
- [Scripts Examples on page 344](#)

Scripts Annotations

Script annotations are used to specify the meta-data of scripts. They are embedded as a part of scripts. They are parsed and stored in space DB while importing/modifying scripts. Annotation is given with the following syntax.

```
/* @[ANNOTATION]= "<ANNOTATION CONTENT>" */
```

The annotation can be given anywhere in the script.

Annotation is used to give the script Context, Name , Description and Confirmation Text of a script.

Annotation	Description
@CONTEXT	Used to give the context in which the script is applicable. When the context is not specified, the default context would be taken as '/device' Refer Context.
@NAME	Used to give the descriptive name of the script.
@DESCRIPTION	Used to give the description of the script.
@CONFIRMATION	Used to give the confirmation text of the script. i.e., what has to be shown when an attempt is made to execute the script. When this field is not provided, no confirmation text will be shown on execution of script. This can be used to provide warnings for certain scripts.
@EXECUTIONTYPE	The type of execution are GROUPEDEXECUTION and SINGLEEXECUTION. When this annotation is not specified, the default option would be SINGLEEXECUTION
@ISLOCAL	Used to define whether the script would be executed locally or would have to be staged on the device. This could be True, False, or /*@ISLOCAL="true"*/
@VARIABLECONTEXT	Used to define the context of a variable.

@PASSSPACEAUTHHEADER	This annotation is specific to local scripts, if the value of this annotation is true, then the script variables \$JSESSIONSSO and \$JSESSIONID would be set. /*@PASSSPACEAUTHHEADER="true"*/
@PASSDEVICECREDENTIALS	This annotation is specific to local scripts. If this annotation is set true, Space sets the device credentials to the variable \$credentials. /*@ PASSDEVICECREDENTIALS ="true"*/

Related Documentation

- [Scripts Overview on page 275](#)

Scripts Examples

The following is the script to take PIC offline.

A script has four associated attributes, @CONTEXT, @NAME, @DESCRIPTION and @CONFIRMATION. These are given within comments (/* */).

The @CONTEXT attribute states, what context the script can be executed on.

The @NAME attribute defines the descriptive name of the script and @DESCRIPTION defines the description of the script.

The @CONFIRMATION defines the text that should be shown to the user for confirmation before the script gets executed. This is to prevent accidental execution of scripts.

```
Version 1.0;
import "../import/junos.xml";
import "cim-lib.slax";

/* Junos Space specific context, name and description */
/* @CONTEXT =
"device-chassis-inventory-chassis-chassis-module[starts-with(name,'PC')]/chassis-sub-module[starts-with(name,'PC')]"
*/
/* @NAME = "Put PIC Offline" */
/* @DESCRIPTION = "Take PIC offline." */
/* @CONFIRMATION = "Are you sure that you want to take the PIC offline?" */
/* @EXECUTIONTYPE = "SINGLEEXECUTION" */
/* @CONFIRMATION = "Are you sure that you want to take the PIC offline?" */
/* Global variables */
var $scriptname = "op-pic-offline.slax";
var $results;
var $regex;
var $result-regex;
var $arguments = {
  <argument> {
    <name> "CONTEXT";
    <description> "The context associated with this script.";
  }
}
param $CONTEXT;
match / {
  <op-script-results> {
```



```

var $regex =
"/device/chassis-inventory/chassis\[name=\"(.*)\"\\]/chassis-module\[name=\"(.*)\"([0-9]+))\"\\]/chassis-sub-module\[name=\"(.*)\"([0-9]+))\"\\\"";
var $result-regex = jcs:regex( $regex , $CONTEXT );
/* Request PIC offline */
var $command = {
  <command> "request chassis pic offline fpc-slot " _ $result-regex[4] _ " pic-slot " _
    $result-regex[6];
}
var $results = jcs:invoke( $command );
/* Error check */
call cim:error-check( $results-to-check = $results , $sev = "external.error" , $script =
  $scriptname , $cmd = $command , $log = "no" );
<output> {
  <HTML> {
    <HEAD> {
      <title> "PIC offline";
      <style type="text/css"> {
        expr "body { font-family: Verdana, Georgia, Arial, sans-serif;font-size:
          12px;color:#fff;}" ;
        expr "td { font-family: Verdana, Georgia, Arial, sans-serif;font-size:
          12px;color:#fff;}" ;
        expr "p { font-family: Verdana, Georgia, Arial, sans-serif;font-size:
          12px;color:#fff;}" ;
      }
    }
    <BODY bgcolor="transparent"> {
      <p> {
        copy-of $results;
      }
    }
  }
}
}
}
}

```

Related Documentation • [Scripts Overview on page 275](#)

PART 6

Reports and Report Definitions

- [Report Definitions on page 349](#)
- [Reports on page 359](#)

CHAPTER 37

Report Definitions

- [Reports Overview on page 350](#)
- [Creating Report Definitions on page 355](#)
- [Managing Report Definitions on page 356](#)

Reports Overview

You can use the Reports workspace to generate customized reports for managing network resources. Reports provide you with the requisite data to monitor the device inventory details, job execution details, and audit trails. You first create a report definition to specify what information to retrieve from the Junos Space Network Management Platform inventory database. You then use this report definition to generate, export, and print the reports. You can use the following pre-defined categories to create report definitions:

- **Audit Trail report definition** – This report definition allows you to view the log activities and tasks initiated on Junos Space Network Management Platform. The following table lists the attributes available with this report definition.

Table 58: Audit Trail Report Definition Attributes

Attribute	Description
User Name	The login ID of the user who initiated the task.
User IP	The IP address of the client computer that the user used to initiate the task.
Task	The name of the task that triggered the audit log.
Timestamp	The UTC time in the database that is mapped to the local timezone of client computer.
Result	The execution result of the task that triggered the audit log.
Job ID	The Job ID of the job-based task that is included in the audit log.
Description	The description of the audit log.

- **Device Inventory report definition** – This report definition allows you to view the generic characteristics of all devices managed by Junos Space Network Management Platform. The following table lists the attributes available with this report definition.

Table 59: Device Inventory Report Definition Attributes

Attribute	Description
Name	The device configuration name for the device.
Consolidated Config State	The state of consolidated configuration for a device.
Vendor	The vendor of the device.
IP Address	The IP address of the device.
Managed Status	The current status of the managed device in Junos Space Network Management Platform.
Device Family	The device family of the selected device.

Table 59: Device Inventory Report Definition Attributes (*continued*)

Attribute	Description
OS Version	The operating system firmware version running on the device.
Platform	The model number of the device.
Serial Number	The serial number of the device chassis.
Connection Status	The connection status of the device - whether UP or DOWN.
Schema Version	The JUNOS configuration schema version on the device.
Authentication Status	The mode of connecting the device to Junos Space Network Management Platform - whether key-based, credentials-based, or a key conflict.
Serial Number	The serial number of the device.
Connection Type	The type of connection between the device and Junos Space Network Management Platform.

- **Device License Inventory report definition** - This report definition allows you to view the generic characteristics of device license information for devices managed by Junos Space Network Management Platform. The following table lists the attributes available with this report definition.

Table 60: Device License Inventory Report Definition Attributes

Attribute	Description
Device Name	The device configuration name for the device.
Feature Name	The name of the licensed SKU or feature.
License Count	The number of times an item has been licensed.
Used Count	The number of times the feature is used.
Need Count	The number of times the feature is used without a license.
Given	The number of instances of the feature that are provided by default.
OS Version	The operating system firmware version running on the device.
Device Family	The device family of the selected device.
Platform	The model number of the device.
Serial Number	The serial number of the device.

- **Device Logical Interface Inventory report definition** - This report definition allows you to view the generic characteristics of the logical interface for devices managed by Junos Space Network Management Platform. The following table lists the attributes available with this report definition.

Table 61: Device Logical Interface Inventory Report Definition Attributes

Attribute	Description
Device Name	The device configuration name for the device.
Physical Interface Name	The name of the physical interface.
Admin Status	Admin status of the interface, whether UP or DOWN.
Link Type	The type of the physical interface link, whether full duplex or half duplex.
Logical Interface IP Address	The IP address of the logical interface.
Logical Interface Encapsulation	The encapsulation used on the logical interface.
VLAN	The VLAN ID of the logical interface.
OS Version	The operating system firmware version running on the device.
Device Family	The device family of the selected device.
Platform	The model number of the device.
Serial Number	The serial number of the device chassis.
Physical Interface IP Address	The IP address of the physical interface.
MAC Address	The MAC address of the physical interface.
Operation Status	The operational status of the interface, whether UP or DOWN.
Physical Interface Encapsulation	The encapsulation used on the physical interface.
Speed	The speed at which the interface is running (in Mbps).
MTU	MTU size
Description	The description of the logical interface.

- **Device Physical Interface Inventory report definition** - This report definition allows you to view the generic characteristics of the logical interface for devices managed by Junos Space Network Management Platform. The following table lists the attributes available with this report definition.

Table 62: Device Physical Interface Inventory Report Definition Attributes

Attribute	Description
Device Name	The device configuration name for the device.
Physical Interface Name	The name of the physical interface.
Admin Status	The admin status of the interface, whether UP or DOWN.
Link Type	The type of the physical interface link, whether full duplex or half duplex.
IP Address	The IP address of the physical interface.
OS Version	The operating system firmware version running on the device.
Device Family	The device family of the selected device.
Platform	The model number of the device.
Serial Number	The serial number of the device chassis.
MAC Address	The MAC address of the physical interface.
Operation Status	The operational status of the interface, whether UP or DOWN.
Encapsulation	The encapsulation used on the physical interface.
Speed	The speed at which the interface is running (in Mbps).
MTU	MTU size
Description	The description of the physical interface.

- **Device Software Inventory report definition** - This report definition allows you to view the generic software package installation information for devices managed by Junos Space Network Management Platform. The following table lists the attributes available with this report definition.

Table 63: Device Software Inventory Report Definition Attributes

Attribute	Description
Device Name	The device configuration name for the device.
Package Name	The name of the installed software package.
Version	The version number of the installed software package.
Type	The type of the installed software package.

Table 63: Device Software Inventory Report Definition Attributes (*continued*)

Attribute	Description
OS Version	The operating system firmware version running on the device.
Device Family	The device family of the selected device.
Platform	The model number of the device.
Serial Number	The serial number of the device chassis.
Model	The model of the device.
Routing Engine	The specific Routing Engine on a device supporting multiple Routing Engines.
Description	The description of the installed software package

- **Job Inventory report definition** - This report definition allows you to view the generic execution characteristics of Junos Space Network Management Platform Jobs. The following table lists the attributes available with this report definition.

Table 64: Job Inventory Report Definition Attributes

Attribute	Description
ID	The numerical ID of the job.
Name	The name of the job is the job type appended with the job ID.
Percent	The percentage of the job that has been completed.
Job Type	The supported job types.
State	The state of job execution.
Summary	The operations executed for the job.
Scheduled Start Time	The start time specified for the job.
User	The login name of the user who scheduled the job.
Recurrence	The model of the device.
Retry Group ID	The specific Routing Engine on a device supporting multiple Routing Engines.
Actual Start Time	The description of the installed software package
End Time	
Previous Retry	

By default, a pre-defined set of attributes are included in a report definition. You can choose to add or remove the attributes according to what information you want from the final generated report. You can group, sort, or filter data based on specific attributes available with the report definition.

You can use the report definitions to generate reports in the CSV, PDF, and HTML format. You can also schedule the delivery of generated reports to a designated SMTP server or a SCP server. You can view, download, or print the generated reports from the Generated Reports page in the Reports workspace.

- Related Documentation**
- [Creating Report Definitions on page 355](#)
 - [Creating Report Definitions on page 355](#)
 - [Generating Reports on page 359](#)

Creating Report Definitions

Report definition specifies what information to retrieve from the Junos Space Network Management Platform inventory database and how this information is displayed in the reports generated using the report definition. You can create report definitions from the Reports workspace. The Report Definitions page in the Reports workspace lists all the report definitions you have created. It also lists the name of the report definition, the user who created the report definition, the time the report definition was created, the description of the report definition, and a link to the reports generated using the report definition.

To create a report definition:

1. Select **Reports > Report Definitions**.
2. Click the Add icon in the menu bar.
The Create Report Definition page is displayed.
3. In the **Report Name** field, enter the name of the report definition.
4. In the **Description** field, enter a description for the report definition.
5. Click the Add icon to add categories to the report definition.
The Select Categories window is displayed.
6. Select the checkboxes next to the categories you want to add to the report definition.
7. Click **Add**.
8. Click the Pencil icon in the Filters column corresponding to the category in which you want to add the column and filter.
The Edit Columns/Filters window is displayed.
9. Select the columns that you want to add to the report definition from the Available column and click the right arrow to move the filters to the Selected column.

10. Select an appropriate option in the **Group By** drop-down menu to group the columns in the report definition in a specific order.
11. Select an appropriate option in the **Sort By** drop-down menu to sort the columns in the report definition in a specific order.
12. Select the appropriate option button next to the Sorting Order section to choose a order of sorting the columns in the report definition.
13. Click the **Add Filter** icon to add filters in the report definition.
14. Select the appropriate column from the drop-down menu for which you want to add a filter.
15. Select the appropriate operand from the drop-down menu.
16. Enter the filtering value in the text field.
17. Click **OK**.
18. Click **Create**.

Related Documentation • [Managing Report Definitions on page 356](#)

Managing Report Definitions

You can view the report definitions you have created on the Report Definitions page. You can modify, clone, delete, and view the report definition details from the Report Definitions page. The Report Definitions page lists the name of the report definition, the user who created the report definition, the time the report definition was created, and the description of the report definition. You can perform the following tasks on a report definition:

- [Modify Report Definitions on page 356](#)
- [Cloning Report Definitions on page 357](#)
- [Deleting Report Definitions on page 357](#)
- [Viewing Report Definitions on page 357](#)

Modify Report Definitions

To modify a report definition:

1. Select **Reports > Report Definitions**.
2. Right-click the report definition you want to modify and select **Modify** from the contextual menu.

The Modify Report Definition page is displayed. You can change all the parameters of the report definition except the Name field.

3. Click **Modify**.

Cloning Report Definitions

To clone a report definition:

1. Select **Reports > Report Definitions**.
2. Right-click the report definition you want to clone and select **Clone** from the contextual menu.

The Clone Report Definition page is displayed. You can change all the parameters of the report definition.

3. Click **Clone**.

Deleting Report Definitions

To delete a report definition:

1. Select **Reports > Report Definitions**.
2. Right-click the report definition you want to delete and select **Delete** from the contextual menu.

The Delete Report Definition window is displayed.

3. Click **Delete**.

Viewing Report Definitions

To view the details a report definition:

1. Select **Reports > Report Definitions**.
2. Right-click the report definition whose details you want to view and select **View** from the contextual menu.

The View Report Definition window is displayed.

3. Click **OK** to close the window.

Related Documentation • [Creating Report Definitions on page 355](#)

CHAPTER 38

Reports

- [Generating Reports on page 359](#)
- [Viewing Generated Reports on page 360](#)
- [Deleting Generated Reports on page 360](#)

Generating Reports

You can generate reports from the report definitions you have created. The different types of reports provided by Junos Space Network Management Platform include, Audit Trail report, Device Inventory report, Device Physical Interface Inventory report, Device Logical Interface Inventory report, Device Licence Inventory report, Device Software Inventory report, and Job Inventory report.

To generate reports:

1. Select **Reports > Report Definitions**.
2. Right-click the report definition that you want to use to create a report and select the Generate Report icon from the menu bar.

The Generate Reports window is displayed.
3. Select the appropriate report types you want to generate by selecting the checkboxes next to the Report Format section.

Junos Space Network Management Platform generates reports in CSV, PDF, and HTML formats.
4. Select the checkbox next to the SCP Server label to configure Junos Space Network Management Platform to store the report in a directory on an SCP server.
5. To configure the SCP server:
 - a. In the **IP Address** field, enter the IP address of the SCP server.
 - b. From the **Port** drop-down menu, select the appropriate port number.
 - c. In the **Directory** field, enter the directory on the SCP server where the reports are stored.
 - d. In the **Username** field, enter the username used to access the SCP server.
 - e. In the **Password** field, enter the username used to access the SCP server.

6. Select the checkbox next to the SMTP Server label to configure Junos Space Network Management Platform to email the report to the email address you specify.
7. Enter the email address in the **Email Address** field.
8. Click **Add**.
9. Click the **Schedule at a later time** checkbox and specify the date and time to schedule the generation of the report at a later point in time.
10. Click the **Recurrence** checkbox and specify the frequency to generate the report periodically.
11. Click **Generate**.

Related Documentation • [Creating Report Definitions on page 355](#)

Viewing Generated Reports

You can view the reports you have generated on the Generating Reports page. You can view the name of the report, the description of the report, the name of the report definition, user who generated the report, the time the report was generated, the formats in which the report is available, the link to view and download the report, and the job ID for the report generated.

To view the reports you have generated:

1. Select **Reports > Generated Reports**.
The list of generated reports are displayed in the tabular format.
2. Click the **View/Download** link for the report you want to view or download.
3. Click the format of the report you want to view and download.

Related Documentation • [Generating Reports on page 359](#)

Deleting Generated Reports

You can delete the reports you have generated on the Generating Reports page.

To delete the reports you have generated:

1. Select **Reports > Generated Reports**.
The list of generated reports are displayed in the tabular format.
2. Select the reports you want to delete and click the Delete icon on the menu bar.
The Delete Report window is displayed.
3. Select the report you want to delete and click **Delete**.

Related Documentation • [Generating Reports on page 359](#)

PART 7

Network Monitoring

- [Network Monitoring Overview on page 365](#)
- [Monitoring Devices and Assets on page 371](#)
- [Working With Events, Alarms, and Notifications on page 387](#)
- [Working With Reports and Charts on page 397](#)
- [Managing Network Monitoring System on page 405](#)
- [Managing Network Monitoring Operations on page 409](#)
- [Managing Devices on page 433](#)
- [Configuring Alarm Notifications on page 435](#)

Network Monitoring Overview

- [Network Monitoring Workspace Overview on page 365](#)
- [Network Monitoring Reports Overview on page 368](#)

Network Monitoring Workspace Overview

The Network Monitoring workspace enables you to assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and diverse other things; for example, whether Service Level Agreements (SLAs) have been violated.



NOTE: Space 13.1 supports SNMP monitoring of devices using SNMP v1/V2c only; SNMPv3 is currently not supported.



CAUTION: Although additional network monitoring functionality can be accessed by customizing its XML files, editing these files can affect the functionality of the Network Monitoring workspace. We recommend that you do not edit these XML files unless you are directed to do so by Juniper Networks.

A Junos Space remote user assigned the FMPM manager role can specify a username and password to access the Network Monitoring workspace. When a remote user (with the FMPM manager role) logs in from the Junos Space user interface, Junos Space authenticates the user from the remote authentication server as follows:

- If the remote authentication is successful, Junos Space uses the user's login credentials to authenticate with the network monitoring server and either creates or updates the network monitoring local user.
- If the remote authentication fails and the user previously existed on the network monitoring server, Junos Space removes the network monitoring local user.

To analyze and aggregate device-level performance data, and to detect device faults, the Network Monitoring workspace uses a collection of data from managed elements.

Performance data is collected automatically if the SNMP settings are set properly for a discovered device.

- *Collection*
 - View historical performance data by using a graphical monitoring tool that allows customization of the parameters to be displayed and the devices to be monitored
 - Create graphs and charts
 - Create and export reports in PDF and HTML formats
 - Define advanced variables that require calculations for historical performance monitoring
 - Allow raw data to be rolled up into processed data, allowing data to be processed from a more-specific to a less-specific level (for example, data collected at a quarter hourly interval can be rolled into hourly data, hourly data can be rolled into daily data, daily can be rolled into weekly data, and weekly data can be rolled into yearly data)
- *Thresholds*
 - Set thresholds for performance data values—including specifying warning and error levels
 - Create threshold graphs
 - Generate threshold-crossing alarms that can be displayed or forwarded
- *Faults*
 - Receive SNMP traps directly from devices and other enterprise management systems (EMSs)
 - Forward traps to other EMSs
 - Generate and display events and alarms
 - Get basic correlation with alarms; for example, clearing alarms, deduplicating alarms
 - Detect device faults based on data collected from devices

You can perform the following tasks from the Network Monitoring workspace:

- Node List: List all the devices under monitoring (see [“Viewing the Node List” on page 371](#))
- Search: Search for devices (see [“Searching in the Network Monitoring Workspace” on page 374](#))
- Outages: View unavailable (down) services (see [“Viewing and Tracking Outages” on page 387](#))
- Events: View events (see [“Viewing and Managing Events” on page 388](#))
- Alarms: View alarms (see [“Viewing and Managing Alarms” on page 119](#))
- Notifications: Display notices received by users (see [“Viewing, Configuring, and Searching for Notifications” on page 395](#))

- Assets: Search asset information and assets inventory (see [“Tracking and Searching for Assets” on page 377](#))
- Reports: View reports (see [“Viewing Reports” on page 398](#))
- Charts: View charts (see [“Viewing Charts” on page 403](#))
- Topology: View nodes in the network topology and the events and alarms associated with the nodes (see [“Working with Topology” on page 378](#))
- Admin: Perform system administration (see [“Admin: Configuring Network Monitoring” on page 405](#))

The main Network Monitoring landing page is a dashboard, displaying the most important information about your nodes:

- Nodes with outages
- Availability over the last 24 hours
- Notifications (outstanding notices)
- On-call schedule
- Key SNMP customized (KSC) performance reports (if defined and available)

In addition, from this page you can do quick searches on nodes and resource graphs.



NOTE: Network Monitoring upgrade customization – Upgrade from previous releases (12.2 or 12.3) to 13.1 allows a means to preserve the custom configuration that might have been performed on XML files from the backend automatically. For example, let us assume that you have modified or customized the SNMP poll interval in the `collectd-configuration.xml` in Junos Space Platform version 12.2 or 12.3, that is, before upgrade to 13.1. When you upgrade to version 13.1, the upgrade process automatically recognizes the changes made and preserves the changes in network monitoring database by renaming the XML file, for example, `collectd-configuration.xml.old`. You can use these preserved, customized configuration files (in this example, `collectd-configuration.xml.old`) to update or replace the new configuration files available after the upgrade.

**Related
Documentation**

- [Network Monitoring Reports Overview on page 368](#)

Network Monitoring Reports Overview

You can generate and view resource graphs, key SNMP customized (KSC) performance reports, KSC node reports, KSC domain reports, database reports, and statistics reports. To access the reports function, select **Network Monitoring > Reports**.

- [Resource Graphs on page 368](#)
- [Key SNMP Customized \(KSC\) Performance Reports, Node Reports, and Domain Reports on page 368](#)
- [Database Reports on page 368](#)
- [Statistics Reports on page 368](#)

Resource Graphs

Resource graphs provide an easy way to represent visually the data collected from managed nodes throughout your network. You can display critical SNMP performance, response time, and so forth.

You can narrow your selection of resources by entering a search string in the Name contains box. This invokes a case-insensitive substring match on resource names.

Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports

KSC reports enable you to create and view SNMP performance data using prefabricated graph types. The reports provide a great deal of flexibility in time spans and graph types. You can save KSC report configurations so that you can refer to key reports in the future.

Node reports show SNMP data for all SNMP interfaces on a node.

Domain reports show SNMP data for all SNMP interfaces in a domain. You can load node reports and domain reports into the customizer and save them as a KSC report.

You can narrow your selection of resources by entering a search string in the Name contains box. This invokes a case-insensitive substring match on resource names.

Database Reports

Database reports provide a graphical or numeric view of your service-level metrics for the current month-to-date, previous month, and last 12 months by categories.

Statistics Reports

Statistics reports provide regularly scheduled statistical reports on collected numerical data (response time, SNMP performance data, and so forth).

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Creating Reports on page 397](#)
- [Deleting Reports on page 403](#)
- [Viewing Reports on page 398](#)

- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)

CHAPTER 40

Monitoring Devices and Assets

- [Viewing the Node List on page 371](#)
- [Resyncing Nodes on page 372](#)
- [Turning SNMP Data Collection Off and On on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)
- [Viewing the Dashboard on page 375](#)
- [Tracking and Searching for Assets on page 377](#)
- [Working with Topology on page 378](#)

Viewing the Node List

Junos Space Network Management Platform is monitored by default using the built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list, and referred to hereafter as the Junos Space Network Management Platform node.

Select **Network Monitoring > Node List**. The Node List page appears. This page displays a list of your nodes and enables you to drill down into each of them.

From the Node List page, you can also access the Resync Nodes subtask (see [“Resyncing Nodes” on page 372](#)).

The Node List page displays a list of all the nodes in your network. You can also display the interfaces for each node. The top level of the Node List displays only the hostname of each device. Click the hostname of the desired device to see:

- SNMP Attributes
- Availability
- Node Interfaces—IP Interfaces, Physical Interfaces (where applicable)
- General (status and detailed information)
- Surveillance Category Memberships
- Notification
- Recent Events
- Recent Outages

Each of these items has links enabling you to drill deeper into the corresponding aspect of the node's performance.

For each node, you can also view events, alarms, outages, asset information, rescan, access the admin options for it, and schedule outages for it.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Viewing and Managing Alarms on page 119](#)
- [Viewing, Configuring, and Searching for Notifications on page 395](#)
- [Tracking and Searching for Assets on page 377](#)

Resyncing Nodes

You should resynchronize your nodes when the contents of the Node List page in the Network Monitoring workspace do not correspond with the device list on the Manage Devices page in the Devices workspace (see [“Viewing Managed Devices” on page 41](#)).

To resynchronize your nodes:

1. Select **Network Monitoring > Node List > Resync Nodes**.
2. Click **Confirm**.

The **Resync Nodes Job Information** dialog box appears.

3. (Optional) To view details of the resynchronization job, click the job ID displayed in the dialog box.
4. Click **OK**.

The Node List page appears, displaying the resynchronized nodes.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Viewing the Node List on page 371](#)
- [Turning SNMP Data Collection Off and On on page 372](#)
- [Viewing Managed Devices on page 41](#)

Turning SNMP Data Collection Off and On

Network performance can be adversely affected by the amount of traffic generated by SNMP data collection. For this reason, SNMP service in Junos Space Network Management Platform is not started by default.

Junos Space Network Management Platform Network Monitoring is always turned on for all devices by default. The ability to turn on data collection is controlled by the

Monitor_SNMP surveillance category. Turning on data collection increases the amount of SNMP traffic, however. If the surveillance category is removed from a device, data collection is turned off.

To turn SNMP data collection off or on for a device:

1. In the Network Monitoring workspace, display the Node List page and click the node name.

The resulting page displays detailed information about the device.

For example, you can select **Network Monitoring > Node List** or you can select **Network Monitoring > Search** and click **All nodes** in the Search for Nodes section of the Search page to display the Node List page.

2. In the Surveillance Category Memberships title bar, click **Edit**.

The Edit surveillance categories on *node name* page appears.

3. Select the **Monitor_SNMP** category from the Categories On Node list on the right.

If this category is *not* in the list on the right, then SNMP data collection is already turned off.

4. Click **Remove** between the two lists.

The removed category appears in the list of Available Categories on the left.

To turn on data collection for selected devices, reverse the process described here.



NOTE: The Network Monitoring functionality performs SNMP data collection by default only on primary interfaces. If you want to change this, instead of manually selecting the interfaces to be monitored from the GUI, you can set data collection for all interfaces by default by modifying the SNMP collection to set the SNMP Storage Flag to all (see [“Managing SNMP Collections” on page 427](#)). For information on the procedure to select other interfaces and the distinction between primary and secondary interfaces, see [“Configuring SNMP Data Collection per Interface” on page 410](#).

Related Documentation

- [Viewing the Node List on page 371](#)
- [Searching in the Network Monitoring Workspace on page 374](#)
- [Viewing the Dashboard on page 375](#)

Searching in the Network Monitoring Workspace

To search for nodes or asset information, use the Search task in the Network Monitoring workspace—select **Network Monitoring > Search**. The Search page has two sections, Search for Nodes and Search Asset Information.

To quickly search for nodes:

- To display the entire node list, click **All nodes** in the Search for Nodes section.
- To display a list of all nodes and their interfaces, click **All nodes and their interfaces** in the Search for Nodes section.
- To display a list of all nodes that have asset information assigned, click **All nodes with asset info** in the Search Asset Information section. The asset information fields are very comprehensive, ranging from address to circuit ID to date installed, to lease expiry date to number of power supplies installed.

You can search for nodes using these criteria:

- **Name containing**—Searching by name is case-insensitive and inclusive. For example, searching on serv would find serv, Service, Reserved, NTSERV, or UserVortex.
 - The *underscore* character (`_`) acts as a single-character wildcard.
 - The *percent* character (`%`) acts as a multiple-character wildcard.
- **TCP/IP address**—Allows you to separate the four octets (fields) of a TCP/IP address into separate searches.
 - A single *asterisk* (`*`) acts as a wildcard for an octet.
 - Ranges are indicated by two numbers separated by a *dash* (`-`)
 - *Commas* (`,`) are used for list demarcation.

For example, the following searches are all valid and would each create the same result set---all TCP/IP addresses from 192.168.0.0 through 192.168.255.255:

- 192.168.*.*
- 192.168.0-255.0-255
- 192.168.0,1,2,3-255.*
- **ifAlias, ifName, or ifDescr contains**—Finds nodes with interfaces that match the given search string. This is a case-insensitive inclusive search similar to the **Name containing** search. To find an exact match, select **equals** instead of **contains**.
- **Providing service**—Finds nodes providing a particular service. To search for a node providing a particular service, select the service from the Providing service list.
- **MAC Address like**—To find interfaces with hardware (MAC) addresses matching the search string, use this case-insensitive partial string match. For example, you can find

all interfaces with a specified manufacturer's code by entering the first 6 characters of the MAC address. Octet separators (dash or colon) are optional.

- **Foreign Source like**—To find a node with a foreign source IDs, use this partial string match.

To quickly search for all nodes with asset information assigned, click **All nodes with asset info**.

You can search for assets using these criteria:

- **Category**—Find assets associated with a particular category.
- **Field**—Search for a specific asset field.
- **Containing text**—Find assets containing the search string. This is a case-insensitive inclusive search similar to the **Name containing** search.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)

Viewing the Dashboard

The Network Monitoring Dashboard displays information about your devices.

To view the dashboard:

1. Select **Network Monitoring > Dashboard**.

The Dashboard page displays the default surveillance view with information about your devices, such as their surveillance categories (which determines whether their data is collected for performance management monitoring).

If your dashboard does not display information about all your nodes, you should resynchronize your nodes. See [“Resyncing Nodes” on page 372](#).

Under the Show all nodes heading, each of the items—Routers, Switches, Security Devices, and Other Devices subdivided into categories (High End, Medium, Low End)—is a link. Click the item of interest to display information about that category of node in the lower section of the page.

The Alarms section displays in the header bar the number of alarms currently displayed, and the total number, for example, 1 to 5 of 59. Scroll up and down the lists of alarms by clicking the << and >> symbols in the Alarms header bar.



NOTE: To refresh the display, you might have to click the scroll symbols, << and >>, in the header bar of the table of interest. For example, if you have been looking at routers, and you want to view the alarms for switches, first select **Switches**, then click << or >> in the Alarms header bar to refresh the display.

Table 65 on page 376 displays the alarms.

Table 65: Alarms Table

Column Heading	Content
Node	Device. Clicking the name of the node takes you to the detailed device information page so that you can examine it more closely.
Description	Brief explanation for the alarm.
Count	Number of the same alarm. When there is more than one, the duplicate is not displayed in a separate row in the table.
First Time	The first time the alarm was triggered.
Last Time	The last time the alarm was triggered.

Table 66 on page 376 displays the notifications.

Table 66: Notifications Table

Column Heading	Content
Node	Device. Clicking the name of the node takes you to the detailed device information page so that you can examine it more closely.
Service	The name of the service for which the notification was sent.
Message	The content of the notification.
Sent Time	The time the notification was sent.
Responder	Person who received the notification.
Response Time	The time it took to respond.

Table 67 on page 377 displays the status of the node.

Table 67: Node Status Table

Column Heading	Content
Node	Device. Clicking the name of the node takes you to the detailed device information page so that you can examine it more closely.
Current Outages	The outages currently in effect, expressed as 1 of 1, for example.
24 Hour Availability	The percentage of time in the last 24 hours when the node actually was available, expressed as 93.391%, for example.

Table 68 on page 377 displays the following:

Table 68: Resource Graphs Table

List Contents	Description
Node <i>name</i>	Names of nodes available.
Information options available for the selected node	Varies, depending on the category of node selected, for example: For routers: SNMP Node Data, SNMP Interface Data, Response Time, BGP Peer, OSPF Area Info For switches: Response Time
Filename of the resource graph selected from the list	Below this the selected graph is displayed.

Related Documentation

- [Turning SNMP Data Collection Off and On on page 372](#)
- [Resyncing Nodes on page 372](#)

Tracking and Searching for Assets

The network monitoring system provides a means for you to easily track and share important information about capital assets in your organization. This data, when coupled with the information about your network that the network monitoring system obtains during network discovery, can be a powerful tool not only for solving problems, but in tracking the current state of equipment repairs as well as network or system-related moves, additions, or changes.

There are two ways to add or modify the asset data stored in the network monitoring system:

- Import the data from another source.
- Enter the data manually.

Once you begin adding data to the network monitoring system's assets inventory page, any node with an asset number (for example, bar code) is displayed on the lower half of

this page, providing you with a one-click mechanism for tracking the current physical status of that device.

If you want to search for particular assets by category, simply select the desired category in the Assets in category list and click **Search** to retrieve a list of all assets associated with that category.

For a complete list of nodes, whether or not they have associated asset numbers, click **All nodes with asset info** link.

**Related
Documentation**

- [Network Monitoring Workspace Overview on page 365](#)
- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)

Working with Topology

All devices discovered in Junos Space Network Management Platform are displayed in the Nodes section of the left pane of the topology map. Linkd is used to discover the network topology. Linkd is an ISO/OSI layer 2/3 network topology discovery daemon. The physical link discovery methods such as LLDP, Bridge, OSPF, and CDP are enabled by default. By default, linkd polls devices every 5 hours and discovers the network topology 30 minutes after the polling.

When you select a link on the topology, the link is displayed in a different color. You can select multiple nodes and services in the nodes and services sections in the left pane by pressing Ctrl. You cannot select multiple devices by pressing Shift. You can also use the semantic zoom functionality on the topology map with the Expand Semantic Zoom Level and Collapse Semantic Zoom Level buttons on the topology map. You can also use the selection tool on the topology map to select the nodes and services.

- [Viewing the Nodes Without Links on page 379](#)
- [Viewing Alarms and Node Details for Selected Nodes on page 379](#)
- [Viewing Nodes with Active Alarms on page 380](#)
- [Managing Alarms Associated with Nodes on page 380](#)
- [Filtering Nodes on page 381](#)
- [Viewing the Topology Map with Different Layouts on page 381](#)
- [Viewing the Details of a Node on page 381](#)
- [Pinging a Node on page 382](#)
- [Viewing the Alarms Associated with the Node on page 382](#)
- [Viewing the Events Associated with the Node on page 383](#)
- [Viewing the Resource Graphs Associated with the Node on page 383](#)
- [Grouping Nodes on page 383](#)

- [Adding Nodes to a Group on page 384](#)
- [Removing a Node from a Group on page 384](#)
- [Viewing the Network Services Across Nodes on page 385](#)
- [Viewing the Details of the Network Service Across Nodes on page 385](#)

Viewing the Nodes Without Links

By default, the topology map does not show the nodes that are not linked to other nodes. To view all the nodes on the topology map:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Select the **View** menu and then clear the **Hide Nodes Without Links** check box.

You can view all the nodes on the topology map regardless of whether they are linked or unlinked.

Viewing Alarms and Node Details for Selected Nodes

To view details for selected nodes:

1. Select **Platform > Network Monitoring > Topology**.

By default, node details for all the nodes display under the **Nodes** tab, and all the alarms associated with the nodes display under the **Alarms** tab.

2. From the topology view, click on each the nodes you want to view.
 - To view alarm details for the selected nodes, select the **Alarms** tab

[Table 69 on page 379](#) describes the information displayed in the columns of the Alarms page.

Table 69: Alarm Details

Field	Description
ID	The alarm ID.
Severity	The severity of the alarm (Critical, Major, Minor, Warning, Normal, or Cleared).
Node	The name of the node.
UEI	The Unique Event Identifier, which is assigned to each event , including those generated by traps.
Count	The Count shows the number of events that were reduced to a single alarm row.
Last Event Time	The most recent date and time when the alarm occurred.
First Event Time	The date and time when the alarm first occurred.

Table 69: Alarm Details (*continued*)

Field	Description
Log Message	The log message associated with the alarm.
	<ul style="list-style-type: none"> To view nodes details for the selected nodes, select the Nodes tab. <p>The following nodes details are displayed:</p> <ul style="list-style-type: none"> ID Foreign Source Foreign ID Label Label Source Last Capabilities Scan Primary interface sysObjectId sysName sysDescription sysContact sysLocation

Viewing Nodes with Active Alarms

To view nodes with active alarms:

1. Select **Platform > Network Monitoring > Topology**.
2. From the topology page, select the nodes for which you want to manage alarms.
3. Select **View > Alarm Status**.

In the topology view, the color of the node icon indicates the highest severity alarm associated with the node. In addition, node icons that display a number indicate the count of outstanding alarms and notices associated with that node.

Managing Alarms Associated with Nodes

To acknowledge, unacknowledge, escalate, or clear the alarms associated with a node:

1. Select **Platform > Network Monitoring > Topology**.
2. From the topology page, select the nodes for which you want to manage alarms.
3. Select the **Alarms** tab.

4. Select the check box to the left of the alarm ID for each alarm listing you want to manage.
5. Select the action (Acknowledge, Unacknowledge, Escalate, or Clear) that you want to perform on the selected alarms.
6. Select **Submit** to complete the action.

Filtering Nodes

To filter the nodes:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. In the Filter text box, enter the text related to the nodes you want to filter.
3. Click **Filter**.

You can view the nodes based on the text you entered in the Filter text box.

Viewing the Topology Map with Different Layouts

To view the topology map with different layouts:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Select the **View** menu and then select the appropriate layout.

By default, the topology map is displayed in the FR layout.

You can view the topology map using the following layouts:

- Circle Layout
- FR Layout
- ISOM Layout
- KK Layout
- Manual Layout
- Real Ultimate Layout
- Spring Layout

Viewing the Details of a Node

To view the details of a node:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. From the Nodes section in the left pane of the topology map, select a node for which you want to view the details.

The topology diagram zooms in to show the node you have selected.

3. Mouse over the node.

You can view the details of the node such as the device name, device description, management IP, and the status of the device.



NOTE: You can also right-click the node and select **Node Info** from the contextual menu to view the details of a node, or you can click the **Device** menu and select **Node Info** to view the details of a node.



NOTE: The node tooltip always displays Status as **Active** or **Managed** even if the node is down.

Pinging a Node

To ping a node:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Right-click the node you want to ping.
3. Select **Ping** from the contextual menu.
4. In the **Number of Requests** field, enter the number of ECHO requests to be sent.
5. In the **Time-Out** field, enter the timeout value of the request.
6. From the **Packet Size** drop down menu, specify the size of the ping packet.
7. (Optional) Select the **Use Numerical Node Names** check box.
8. Click **Ping**.

The node is pinged with the specified values and the result of the ping request is displayed.



NOTE: You can also click the **Device** menu and select **Ping** to ping a node.

Viewing the Alarms Associated with the Node

To view the alarms associated with the node:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Right-click the node whose alarm associations you want to view.
3. Select **Events/Alarms** from the contextual menu.

The events and alarms associated with the node are displayed.

4. Select the **Alarms** tab to view only the alarms associated with the node.

You can view the alarms associated with the node.



NOTE: You can also click the **Device** menu and select **Events/Alarms** to view the alarms associated with the node.

Viewing the Events Associated with the Node

To view the events associated with the node:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Right-click the node whose event associations you want to view.
3. Select **Events/Alarms** from the contextual menu.

The events and alarms associated with the node are displayed.

4. Select the **Events** tab to view only the events associated with the node.

You can view the events associated with the node.



NOTE: You can also click the **Device** menu and select **Events/Alarms** to view the events associated with a node.

Viewing the Resource Graphs Associated with the Node

To view the resource graphs associated with the node:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Right-click the node whose resource graphs you want to view.
3. Select **Resource Graphs** from the contextual menu.

The resource graphs associated with the node are displayed. The node resources are shown, such as SNMP node data, SNMP interface data, response time, BGP peers, and OSPF area information.

4. Select the resources for which you want to view the graphs and click **Graph Selection**.



NOTE: You can also use the **Select All** and **Graph All** options to view the resource graphs for all node resources, and you can click the **Device** menu and select **Resource Graphs** to view the resource graphs associated with a node.

Grouping Nodes

To create a group and add nodes to the group:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. On the topology map, select the nodes you want to group and select the **View** menu.

3. Select **Create Group**.

The Create Group pop-up window is displayed.

4. Enter a name for the group in the Group Label field.
5. Click **OK**.

The new group is displayed in the nodes section. You can expand the group to view the nodes in the group.



NOTE: You can rename or delete the group by right-clicking and choosing the Rename Group or Delete Group options from the contextual menu, respectively.



NOTE: Currently the topology feature allows creating duplicate group names.

Adding Nodes to a Group

To add nodes to a group:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. On the topology map, select the nodes you want to add a to group and right-click.
3. Select **Add Item to Group** from the contextual menu.

The Add Item to Group pop-up window is displayed.

4. Select the group from the Group drop-down menu.
5. Click **OK**.

Removing a Node from a Group

To remove a node from a group:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. On the topology map, select the appropriate group and right-click.
3. Select **Remove Item to Group** from the contextual menu.

The Remove Item from Group pop-up window is displayed.

4. Select the node you want to remove from the Item drop-down menu.
5. Click **OK**.

Viewing the Network Services Across Nodes

You can view the network services configured using Junos Space Network Activate across nodes.

To view the network services:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Select the **Services** section at the bottom of the left pane of the topology map.

All services configured using Junos Space Network Activate are displayed.

3. Click a service.

The corresponding links are highlighted on the topology map.

Viewing the Details of the Network Service Across Nodes

To view the details of a network service across nodes:

1. Select **Network Management Platform > Network Monitoring > Topology**.
2. Select the **Services** section at the bottom of the left pane of the topology map.
3. Click a service whose details you want to view.

You can also select multiple services if you want to view the details of multiple services.

4. Mouse over the corresponding link.

You can view the details such as service name and the IDs of the end nodes associated with the service.

- Related Documentation**
- [Network Monitoring Workspace Overview on page 365](#)
 - [Resyncing Nodes on page 372](#)

CHAPTER 41

Working With Events, Alarms, and Notifications

- [Viewing and Tracking Outages on page 387](#)
- [Viewing and Managing Events on page 388](#)
- [Viewing and Managing Alarms on page 391](#)
- [Viewing, Configuring, and Searching for Notifications on page 395](#)

Viewing and Tracking Outages

To track outages, discovered services are polled. If a service does not respond, a service outage is created, which in turn creates notifications.

To view and track outages, select **Network Monitoring > Outages**.

To get details for a particular outage, enter its ID in the Outage ID box and click **Get details**.

Alternatively, to view all outages still extant, click **Current outages**. To view both current and resolved outages, click **All outages**.

To view other outage types from these Outages pages, change the display by selecting from the Outage type list. You can sort on each of these column headings by clicking them:

- ID
- Node
- Interface
- Service
- Down
- Up

You can also return to the results by clicking **Bookmark Results**. Your browser's favorite or bookmark dialog box opens.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Viewing the Node List on page 371](#)

- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)

Viewing and Managing Events

Junos Space Network Management Platform is monitored by default using the built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Management Platform > Network Monitoring > Node List), and referred to hereafter as Junos Space node].

Events signal network or systems-related issues. Acknowledging an event enables you to take responsibility for resolving the problem that triggered it. All events are visible to all users. By default, the Events page displays outstanding, or unacknowledged, events.

The Events task contains the functions described below.

The breadcrumbs at the top of each of these pages contain links taking you back to previous pages. Listings frequently extend over multiple pages, between which you can navigate using the **First**, **Previous**, and **Next** links at the top and bottom left of the pages. On the bottom left of the pages is the number of events on the page, and the number of results on the current page out of the total list.

You can sort on each of the column headings on list pages. You can also return to the results by clicking **Bookmark Results**. Your browser's favorite or bookmark dialog box opens.

- [Events Landing Page on page 388](#)
- [Advanced Event Search on page 388](#)
- [Viewing the Events List on page 389](#)
- [Viewing Event Details on page 390](#)

Events Landing Page

To search for, view, query, or acknowledge events, select **Network Monitoring > Events**.

- To view all events, click **All events** in the Event Queries section, below and to the left of the Event ID field. The Events page appears with the list of unacknowledged events. See "[Viewing the Events List on page 389](#)".
- To get details for a particular event, enter its ID in the Event ID field and click **Get details**. The Event *event ID* section appears. See "[Viewing Event Details on page 390](#)".
- To perform an advanced search, click **Advanced Search** to go to the Advanced Event Search section. The Advanced Event Search section can be used to search the event list on multiple fields. See "[Advanced Event Search on page 388](#)".

Advanced Event Search

Enter values into any of the following fields to narrow down the search:

- Event Text Contains
- Node Label Contains
- TCP/IP Address Like
- Severity

For a service, select from the Service list.

To select events by time, first select the box for the time range that you want to limit.

To select events in a time period, select both boxes and then select the beginning and end of the range time from the lists.

You can determine the order in which found events are displayed by selecting from the Sort By list.

Determine the quantity of events displayed by selecting from the Number of Events Per Page list.

Viewing the Events List

Select **Network Monitoring > Events** and click **All events** in the Event Queries section to display a list of events. By default, the Events page displays outstanding events.

- To see all events, click **View all events** at the top of the page. Clicking Advanced Search takes you to the Advanced Event Search section (see [“Advanced Event Search” on page 388](#)).
- To see the acknowledged events, click the **[-]** (minus sign) in the Search constraints box to toggle between acknowledged and outstanding events. To revert to the outstanding events, click the **[-]** again.

The Events page displays the following information for each event:

- **Ack**—Acknowledge check box. Select this to take responsibility for the issue. If an event has been acknowledged in error, you can toggle the Search constraints box to display acknowledged events, find the event, and unacknowledge it, displaying it again to all users.
- **ID**—Event ID. Click for details, which are displayed in the Event *event ID* section (see [“Viewing Event Details” on page 390](#)).
- **Severity**—See degrees of event severity.
- **Time**—Time when the event occurred. You can choose to view only events occurring before or after the selected event by clicking the **<** or **>** symbol next to the time.
- **Node**—The name of the node is a link targeting the node's details from the Nodes section (see [“Searching in the Network Monitoring Workspace” on page 374](#)). You can choose to view only events on the same node, or to view all events except those on the selected node.
- **Interface**—The IP address of the interface where the event took place. The IP address is a link targeting the interface's details on the Nodes and their Interfaces section (see

[“Searching in the Network Monitoring Workspace” on page 374](#)). You can choose to view only events on the same interface as the selected event, or view all events except those on that interface.

- **Service**—The name of the service affected, where applicable.
- **UEI**—[Unique Event Identifier] You can choose to view only events with the same UEI or all events except those with the same UEI. You can also edit notifications for the event by clicking on the link of that name, which takes you to the Build the rule section for notifications (see [“Configuring Notifications” on page 416](#)).
- **Log message**—The log message.

Viewing Event Details

Select **Network Monitoring > Events**, enter its ID in the Event ID field and click **Get details**. The Event *event ID* section displays the following items:

- **Severity**—Severity of event. Degrees of severity are color-coded and labeled:
 - **CRITICAL**: Numerous devices are affected; fixing the problem is essential.
 - **MAJOR**: Device is completely down or in danger of going down. Immediate attention required.
 - **MINOR**: Part of a device (service, interface, power supply, and so forth) has stopped. Attention required.
 - **WARNING**: Might require action. Should possibly be logged.
 - **INDETERMINATE**: No severity could be associated.
 - **NORMAL**: Informational message. No action required.
 - **CLEARED**: Indicates that a prior error condition has been corrected and service is restored.
- **Time**—Time when event occurred.
- **Node and Interface**—Both of these values are clickable, targeting the Nodes section and the Nodes and their interfaces section respectively on the Search page.
- **Acknowledged By and Time Acknowledged**—Acknowledger of event and the time of acknowledgement.
- **Service**—Service affected, where applicable.
- **UEI**— Unique Event Identifier. UEIs enable disk usage to be handled differently from other events with high-threshold types, which means you can choose to be notified by e-mail of high disk usage only, instead of getting notified of all events of the threshold type high.
- **Log Message**—The full error message.
- **Description**—The explanation for the log message.
- **Operator Instructions**—Instructions for resolving the issue that triggered the event, if available.

- Related Documentation**
- [Network Monitoring Workspace Overview on page 365](#)
 - [Viewing the Node List on page 371](#)
 - [Viewing Managed Devices on page 41](#)
 - [Resyncing Nodes on page 372](#)
 - [Searching in the Network Monitoring Workspace on page 374](#)

Viewing and Managing Alarms

Junos Space Network Management Platform is monitored by default using built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Management Platform > Network Monitoring > Node List), and referred to as Junos Space Network Management Platform node.

There are two basic categories of alarm: acknowledged and outstanding. Acknowledging an alarm indicates that you have taken responsibility for addressing the corresponding network or systems-related issue. Any alarm that has not been acknowledged is considered outstanding and is therefore visible to all users on the Alarms page, which displays outstanding alarms by default.

If an alarm has been acknowledged in error, you can find the alarm and unacknowledge it, making it available for someone else to acknowledge.

When you acknowledge, clear, escalate, or unacknowledge an alarm, this information is displayed in the alarm's detailed view. You can click the alarm ID to view fields such as Acknowledged By, Acknowledgement Type, and Time Acknowledge. These fields display details such as who acknowledged, cleared, escalated, or unacknowledged the alarm; the acknowledgement type (acknowledge, clear, escalate, or unacknowledge); and the date and time the action was performed on the alarm.



NOTE: If a remote user has cleared, acknowledged, escalated, unacknowledged an alarm, the detailed alarm view displays *admin* instead of the actual remote user in the Acknowledged By field.

When you purge alarms, the selected alarms and all corresponding alarm history is purged from the database.

You can search for alarms by entering an individual ID on the initial Alarms page, or by sorting by the column headings on the Alarms page that displays alarms.

- [Viewing Alarms on page 392](#)
- [Acknowledging Alarms on page 393](#)
- [Clearing Alarms on page 394](#)
- [Escalating Alarms on page 394](#)

- [Unacknowledging Alarms on page 394](#)
- [Viewing Acknowledged Alarms on page 394](#)

Viewing Alarms

To view alarms:

1. Select **Network Monitoring > Alarms**.
2. Select one of the following links:
 - All alarms (summary)
 - All alarms (detail)
 - Advanced Search

The Alarms page appears with the list of alarms. By default, the first view for all alarms, both summary and details, shows outstanding alarms, as indicated by the content of the Search constraints box.

3. (Optional) Use the toggle control (the minus sign) in the Search constraints box to show acknowledged alarms.
4. (Optional) You can refine the list of alarms by either or both of the following:
 - Entering information in the Alarm text box.
 - Selecting a time period from the Time list. You can choose only time spans ending now, for example, Last 12 hours.

Select **Search**.

5. (Optional) To view the alarm history for an alarm, select the alarm ID. The alarm history displays the details of previous event or alarm occurrences that map to the event UEI, node ID, IP address, and ifindex of the selected alarm. In addition, when clearing, acknowledging, escalating, or unacknowledging alarms, the alarm action details are also displayed for the corresponding alarms.

The Alarm history provides the following details:

- Event ID
- Alarm ID
- Creation Time
- Severity
- Operation Time
- User
- Operation

Links at the top of the page, under the title, provide access to further functions:

- View all alarms
- Advanced Search

- Long Listing/Short Listing

Table 24 on page 121 describes the information displayed in the columns of the Alarms page. An X indicates that the data is present in the Short Listing or Long Listing displays.

Table 70: Information Displayed in the Alarms List

Data	Short Listing	Long Listing	Comments
Ack check box	X	X	
ID	X	X	Click the ID to go to the Alarm alarm ID section of the Alarms page.
Severity	Color-coding only	X	Toggle enables you to show only alarms with this severity, or not to show alarms with this severity.
UEI		X	Toggle enables you to show only events with this UEI, or not to show events with this UEI.
Node	X	X	Toggles enable you to show only alarms on this IP address, or not to show alarms for this interface.
Interface		X	
Service		X	
Count	X	X	Click the count to view the Events page for the event that triggered this alarm.
Last Event Time	X	X	Mouse over this to see the event ID. Toggles enable you to show only alarms occurring after this event, or only alarms occurring before this event.
First Event Time		X	
Log Msg	X	X	

- Severity Legend—Click to display a table in a separate window showing the full explanations and color coding for the degrees of severity.
- Acknowledge/Unacknowledge entire search—Click to perform the relevant action on all alarms in the current search, including those not shown on your screen.

Acknowledging Alarms

To acknowledge an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Acknowledge Alarms** from the list on the left, and click **Go**.

The alarm is removed from the default view of all users.

Clearing Alarms

To clear an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Clear Alarms** from the list on the left, and click **Go**.

Escalating Alarms

To escalate an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Escalate Alarms** from the list on the left, and click **Go**.

The alarm is escalated by one level.

3. (Optional) To view the severity to which an alarm has been escalated, click the alarm's ID.

Unacknowledging Alarms

To unacknowledge an alarm:

1. Display the list of acknowledged alarms by toggling the Search constraint box so that it shows Alarm is acknowledged.
2. Select the **Ack** check box of the alarm you acknowledged in error. To select all alarms, at the bottom of the page, click **Select All**.
3. At the bottom of the page, select **Unacknowledge Alarms** from the list on the left, and click **Go**.

The alarm appears again in the default view of All Alarms.

Viewing Acknowledged Alarms

To view acknowledged alarms:

1. Select **Network Monitoring > Alarms** and click **All Alarms (summary)** or **All Alarms (details)**.

The Alarms page appears listing the alarms.

2. In the Search constraints field, click the minus sign to toggle between acknowledged and outstanding alarms.
3. (Optional) To remedy an alarm acknowledged by mistake, unacknowledge it.

Related Documentation

- [Viewing, Configuring, and Searching for Notifications on page 395](#)

Viewing, Configuring, and Searching for Notifications

When the system detects important events, one or more notices are sent automatically to configured notification information (such as a pager, an email address, or other notification methods). In order to receive notices, users must have their notification information configured in their user profile (see [“Admin: Configuring Network Monitoring” on page 405](#)), notices must be switched on, and an important event must be received.

Select **Network Monitoring > Notifications**. From the Notifications page, you can:

- Display all unacknowledged notices sent to your user ID by clicking **Your outstanding notices**.
- View all unacknowledged notices for all users by clicking **All outstanding notices**.
- View a summary of all notices sent and acknowledged for all users by clicking **All acknowledged notices**.
- Search for notices associated with a specific user ID by entering that user ID in the User field and clicking **Check notices**.
- Jump immediately to a page with details specific to a given notice identifier by entering that numeric identifier in the Notice field and clicking **Get details**.



NOTE: Getting details is particularly useful if you are using a numeric paging service and receive the numeric notice identifier as part of the page.

- [Notification Escalation on page 395](#)

Notification Escalation

Once a notice is sent, it is considered outstanding until someone acknowledges receipt of the notice using the Notice *notice ID* section of the Notifications page. Select **Network Monitoring > Notifications**, enter a notice ID in the Notice field, click **Get details**, and click **Acknowledge**.

If the event that triggered the notice was related to managed network devices or systems, the Network/Systems group is notified, one by one, with a notice sent to the next member on the list only after 15 minutes has elapsed since the last message was sent.

This progression through the list, or escalation, can be stopped at any time by acknowledging the notice. Note that this is not the same as acknowledging the *event* that triggered the notice. If all members of the group have been notified and the notice has not been acknowledged, the notice is escalated to the Management group, where all members of that group are notified simultaneously (with no 15 minute escalation interval). For details on configuring groups, see [“Admin: Configuring Network Monitoring” on page 405](#).

- Related Documentation**
- [Network Monitoring Workspace Overview on page 365](#)
 - [Viewing the Node List on page 371](#)
 - [Viewing Managed Devices on page 41](#)
 - [Resyncing Nodes on page 372](#)
 - [Searching in the Network Monitoring Workspace on page 374](#)

CHAPTER 42

Working With Reports and Charts

- [Creating Reports on page 397](#)
- [Viewing Reports on page 398](#)
- [Deleting Reports on page 403](#)
- [Viewing Charts on page 403](#)

Creating Reports

You can configure key SNMP customized (KSC) performance reports, node reports, domain reports by selecting **Network Monitoring > Reports**.

- [Creating Key SNMP Customized Performance Reports, Node Reports, Domain Reports on page 397](#)
- [Creating a New KSC Report from an Existing Report on page 398](#)

Creating Key SNMP Customized Performance Reports, Node Reports, Domain Reports

To create a new KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. From the Node and Domain Interface Reports section, select a resource for the report.
3. Under the Customized Reports section, click **Create New > Submit**

The Customized Report Configuration page is displayed.

4. In the Title text box, enter a name for the report.
5. (Optional) To add a graph to the report:
Select **Add New Graph**.
 - a. Select a resource from the Resources section.
 - b. Select **Choose Child Resource** to select the resource you want to use in a graph.
 - c. Select the check box for the specific node resources you want to view, or click **Select All** to select all the displayed node resources.
6. (Optional) To allow global manipulation of the report timespan, select **Show Timespan Button**.

7. (Optional) To allow global manipulation of report prefabricated graph type, select **Show Graphtype Button**
8. (Optional) Select the number of graphs to show per line in the report.
9. To save the report, click **Save**.

Creating a New KSC Report from an Existing Report

To create a new KSC report from an existing report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. Under the Resources section, select the KSC report that you want to use to create a new report and click **Create New from Existing > Submit**.

The Customized Report Configuration page is displayed.

3. Select a resource.
4. In the Title text box, enter a new name for the report.
5. (Optional) Customize the report by adding graphs and specifying the number of graphs per line.
6. Click **Save**.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Network Monitoring Reports Overview on page 368](#)
- [Viewing Reports on page 398](#)
- [Deleting Reports on page 403](#)
- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)

Viewing Reports

Select **Network Monitoring > Reports** to view the following types of reports:

- Resource graphs that provide SNMP performance data collected from managed nodes on your network
- Key SNMP customized (KSC) performance reports, node reports, domain reports. You can generate KSC reports to view SNMP performance data using prefabricated graph types.
- Database reports that provide graphical or numeric views of service level metrics
- Statistics reports that provide regularly scheduled reports on response time, SNMP node-level performance and interface data, and OSPF area data

Viewing Resource Graphs

To view a resource graph:

1. Select **Network Monitoring > Reports > Resource Graphs**.
2. Select the resource node for which you want to generate a standard performance report or custom performance report.
The Node Resources page is displayed.
3. To select the specific node resources data that you want to view, choose one of the following options:
 - To view data for a subset of node resources:
 - a. Click the **Search** option
 - b. Enter a text string to identify the node resources you want to view.
 - c. Click **OK**.
 - d. Select the check box for the specific node resources you want to view, or click **Select All** to select all the displayed node resources.
 - To view data for all listed node resources, click **Select All**.
4. To display graphical data for the all the selected node resources, click **Graph Selection**.
5. In the Time Period field, specify the period of time (last day, last week, last month, custom) which the report should cover.

The statistical data is refreshed to reflect the time period specified.

Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, Domain Reports

To view a KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. Select the resource node for which you want to view a standard performance report or custom performance report.
The Custom View Node Report is displayed.
3. (Optional) To customize the Node Report view:
 - To override the default time span, in the Override Graph Timespan list, select number of hours, days, or months, or select by quarter, or year.
 - To override the default graph type, from the Override Graph type list, select number of hours, days or months, by quarter or by year.
4. Select **Update Report View** to refresh the report.
5. Select **Exit Report Viewer** to exit the report view or select **Customize This Report** to make additional updates to the report.

Viewing Database Reports

To view database reports:

1. Select **Network Monitoring > Reports > Database Reports > List reports**.

The Local Report Repository page is displayed.

2. Select on a report page number or select **Next** or **Last** to scroll through the available reports to locate the database report you want to view.
3. To execute a report, from the row that lists the report, select the arrow icon from the Action column.

The Run Online Report page is displayed.

4. In the Report Format field, select either PDF or comma-separated values (CSV) format for the report from the list.
5. Select **run report**.

For PDF, the report is displayed in the selected format. For CSV, you are prompted to either open or save the file.

Sending Database Reports

To send database reports:

1. Select **Network Monitoring > Reports > Database Reports > List reports**.

The Local Report Repository page is displayed.

2. Select on a report page number or select **Next** or **Last** to scroll through the available reports to locate the database report you want to send.
3. You can send a report to file system or e-mail the report.

- To execute a report, in the row that lists the report, select the arrow icon from the Action column.

The Run Online Report page is displayed.

- a. From the Report Format list, select either PDF or comma-separated values (CSV) format for the report from the list.
- b. Select **run report**.

For PDF, the report is displayed in the selected format. For CSV, you are prompted to either open or save the file.

- To send a report to a file system or e-mail the report, select the Deliver report icon from the Action column.

The Report Parameters page is displayed.

- a. From the report category field, select a category (Network Interfaces, Email Servers, Web Servers, Database Servers, and so forth)
- b. From the end date field, select the end date and time for the report.
- c. Select **Proceed**.
The Report Delivery Options page is displayed.
- d. In the name to identify this report field, specify a name for the report.
- e. (Optional) To send the report through e-mail, select the email report check box.
- f. In the format field, select the format type (HTML, PDF, SVG).
- g. In the recipient field, enter the name of the person to whom the report will be sent.
- h. (Optional) To save a copy of the report select the **save a copy of this report** check box.
- i. Select **Proceed**.
The Report Running page is displayed.
- j. Select **Finished** to close the page and return to the Local Report Repository page.

Viewing Pre-run Database Reports

To view database reports:

1. Select **Network Monitoring > Reports > Database Reports > View and manage pre-run reports**.
All the pre-run reports are displayed in a table.
2. From the view report column, select the **HTML**, **PDF**, or **SVG** link to specify the format in which you want to view the report.
The database report is displayed.

Viewing Statistics Reports

To view statistics reports:

1. Select **Network Monitoring > Reports > Statistics Reports**.
The Statistics Report List page displays a list of all available reports in a table.
2. To search for specific information in statistics reports, enter search text in the blank field directly above a Statistics Report column, and select **Filter**.
All available statistics reports that match the filter text you specified are displayed in the Statistics Report List page.

3. To clear the filtered information and restore the original list of statistics reports, select **Clear**.

All available statistics reports are again displayed in the Statistics Report List page.

4. To view complete information for a specific statistics report, click the Report description link from the Statistics Report List page.

The statistics report is displayed and includes Parent resources and resource graphs with SNMP interface data.

Generating a Statistics Report for Export

To generate a statistics report as a PDF file or Excel spreadsheet:

1. Select **Network Monitoring > Reports > Statistics Reports**.

The Statistics Report List page displays a list of all available reports in a table.

2. In the Report Description column, select the report link.

The statistics report is displayed and includes all information for that report, including parent resources and resource graphs with SNMP interface data.

3. Choose PDF or Excel as the format for the statistics report:

- To generate the statistics report in PDF format, in the top-right corner of the Statistics Report, select the Export PDF icon.

The File Download window is displayed.

- To generate the statistics report as an Excel spreadsheet, in the top-right corner of the Statistics Report, select the Export Excel icon.

The File Download window is displayed.

4. From the File Download window, select **Open** to view the statistics report or select **Save** to save the statistics report.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Network Monitoring Reports Overview on page 368](#)
- [Creating Reports on page 397](#)
- [Deleting Reports on page 403](#)
- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)

Deleting Reports

To delete key SNMP customized (KSC) reports and database reports, select **Network Monitoring > Reports**.

- [Deleting Key SNMP Customized Reports on page 403](#)
- [Deleting Pre-run Database Reports on page 403](#)

Deleting Key SNMP Customized Reports

To delete a KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. From the Customized Reports section, select the report that you want to delete.
3. Select the **Delete** radio button.
4. Select **Submit**.

The KSC report is deleted.

Deleting Pre-run Database Reports

To delete a database report:

1. Select **Network Monitoring > Reports > View and manage pre-run reports**.
All the pre-run reports are displayed in a table.
2. From the select column in the reports table, select the check box for the database report that you want to delete.
3. Select **delete checked reports**.

The database report is deleted.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Network Monitoring Reports Overview on page 368](#)
- [Creating Reports on page 397](#)
- [Viewing Reports on page 398](#)
- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)

Viewing Charts

To view charts, select **Network Monitoring > Charts**.

This page displays by default:

- Alarms Severity Chart, showing the counts of both alarms and events, distinguishing between major, minor, and critical severities.
- Last 7 Days Outages, showing the counts of outages per service.
- Node Inventory, showing the counts of nodes, interfaces, and services.

Managing Network Monitoring System

- [Admin: Configuring Network Monitoring on page 405](#)

Admin: Configuring Network Monitoring

You can view and modify information about Junos Space Network Monitoring users including their name, notification information, and duty schedules. This topic contains the following tasks:

- [Modifying Users on page 405](#)
- [Network Monitoring System: System Information on page 406](#)
- [Notification Status on page 407](#)

Modifying Users

To modify a user:

1. Select **Network Monitoring > Admin > Configure Users**.
Click the User ID link to view detailed information about a user.
2. (Optional) To modify a user, select on the edit icon from the Modify column.
The Modify User page appears.
3. (Optional) Add any necessary details to the user profile.



NOTE: Even if you do not add details, you must click **Finish** to modify a user.

- Full Name
- Comments
- Telephone PIN
- Email
- Pager Email
- XMPP Address (for instant messages using the Jabber XMPP protocol)

- Microblog Username
- Numeric Service (for pagers that cannot display text messages)
- Numerical PIN — The Telephone PIN is an optional numeric field used to authenticate called users.
- Text Service (for alphanumeric pagers)
- Text PIN
- Work Phone
- Mobile Phone
- Home Phone
- Duty Schedules

Duty schedules determine when users should receive notifications. A duty schedule consists of a list of days for which the time applies and a time range (military time: days run from 0000 to 2359). If your duty schedules span midnight, or if your users work multiple, non-contiguous time periods, configure multiple duty schedules. To do this, select the number of duty schedules to add from the drop-down box next to **Add This Many Schedules**, and click **Add This Many Schedules**. To create a duty schedule spanning midnight, enter the first schedule from the start time to 2359 on one day, and enter a second duty schedule that begins at 0000 and ends at the end of that user's coverage. To remove configured duty schedules, select the appropriate check boxes in the Delete column and click **Remove Checked Schedules**.

4. (Optional) Edit any necessary details in the user profile.
5. Click **Finish**.

Network Monitoring System: System Information

Select **Network Monitoring > Admin > System Information** to view the network monitoring configuration and the system configuration on which network monitoring is running.

- The network monitoring Configuration section of the page lists the following information:
 - Version
 - Home Directory
 - RRD store by Group—true or false
 - Web-Application Logfiles—location
 - Reports directory—location
 - Jetty http host
 - Jetty http port—usually 8980
 - Jetty https host
 - Jetty https port
- The System Configuration section of the page lists the following information:

- Server Time
- Client Time
- Java Version
- Java Virtual Machine
- Operating System
- Servlet Container
- User Agent

Notification Status

Notifications are sent out only if Notification Status is switched to On. This is a system wide setting. The default setting is Notification Status Off. After you change the setting, click **Update**.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)
- [Viewing the Node List on page 371](#)
- [Viewing Managed Devices on page 41](#)
- [Resyncing Nodes on page 372](#)
- [Searching in the Network Monitoring Workspace on page 374](#)
- [Viewing Charts on page 403](#)

Managing Network Monitoring Operations

- [Configuring SNMP Community Names by IP on page 409](#)
- [Configuring SNMP Data Collection per Interface on page 410](#)
- [Managing and Unmanaging Interfaces and Services on page 411](#)
- [Managing Thresholds on page 411](#)
- [Selecting and Sending an Event to the Network Management System on page 415](#)
- [Configuring Notifications on page 416](#)
- [Configuring Scheduled Outages on page 419](#)
- [Compiling SNMP MIBs on page 420](#)
- [Managing Events Configuration Files on page 425](#)
- [Managing SNMP Collections on page 427](#)
- [Managing Data Collection Groups on page 428](#)

Configuring SNMP Community Names by IP

This task enables you to configure SNMP community names by IP address. You also need to configure the community string used in SNMP data collection. The network monitoring functionality is shipped with the *public* community string. If you have set a different *read* community on your devices, this is where you must enter it.

In the boxes on the left, enter in a specific IP address and community string, or a range of IP addresses and a community string, and other SNMP parameters. The network monitoring functionality optimizes this list, so enter the most generic first (that is, the largest range) and the specific IP addresses last, because if a range is added that includes a specific IP address, the community name for the specific address is changed to be that of the range. For devices that have already been discovered and that have an event stating that data collection has failed because the community name changed, you might need to update the SNMP information on the interface page for that device (by selecting the Update SNMP link) for these changes to take effect.

To configure SNMP using an IP address:

1. Select **Network Monitoring > Admin > Configure SNMP Community Names by IP**, and enter in the First IP Address field either a single IP address, or the first one of a range.
2. If you are not entering a range of IP addresses, leave the Last IP Address field blank, otherwise enter the last IP address of the range.
3. In the Community String field, enter the community string you use for your devices. The default is *public*.
4. (Optional) Enter a timeout in the Timeout field.
5. Select the appropriate version from the Version list.
6. (Optional) Enter the number of retries in the Retries field.
7. (Optional) Enter the port number in the Port field.
8. Click **Submit**. The system displays a message telling you whether network monitoring needs to be restarted for the configuration to take effect.

Configuring SNMP Data Collection per Interface

For each different SNMP collection scheme, there is a parameter called SNMP Storage Flag. If this value is set to primary, then only values pertaining to the node as a whole or the primary SNMP interface are stored in the system. If this value is set to all, then all interfaces for which values are collected are stored. If this parameter is set to select, then the interfaces for which data is stored can be selected. By default, only information from primary and secondary SNMP interfaces are stored.

You can choose other non-IP interfaces on a node if you have set up the SNMP collection.

To manage SNMP data collection for each interface:

1. Select **Network Monitoring > Admin > Configure SNMP Data Collection per Interface**.
The Manage SNMP Data Collection per Interface page appears.
2. Select the node for which you want to manage data collection.
The Choose SNMP Interfaces for Data Collection page appears listing all known interfaces.
3. Select the appropriate value for the interface in the Collect column.
Primary and secondary interfaces are always selected for data collection.

Related Documentation

- [Managing SNMP Collections on page 427](#)

Managing and Unmanaging Interfaces and Services

To manage a service, you must manage its interface. The Manage and Unmanage Interfaces and Services page enables you to manage not only interfaces, but also the combination of node, interface, and service. The tables on this page display the latter, with the Status column indicating if the interface or service is managed or not.

Managing an interface or service means that the network monitoring functionality performs tests on this interface or service. If you want to explicitly enable or disable testing you can set that up here. A typical case is if a webserver is listening on both an internal and an external interface. If you manage the service on both interfaces, you will get two notifications if it fails. If you want only one, unmanage the service on one of the interfaces.

Select **Network Monitoring > Admin > Manage and Unmanage Interfaces and Services** to manage or unmanage your node, interface, and service combinations.

To change the status, you have these choices: **Apply Changes**, **Cancel**, **Select All**, **Unselect All**, or **Reset**.

Managing Thresholds

Thresholds allow you to define triggers against any data retrieved by the SNMP collector, and generate events, notifications, and alarms from those triggers. You can add, remove, and modify thresholds.

- [Creating Thresholds on page 411](#)
- [Modifying Thresholds on page 414](#)
- [Deleting Thresholds on page 415](#)

Creating Thresholds

To create a threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

The Edit group page appears.

3. Select **Create New Threshold**.

The Edit threshold page appears.

4. To configure the threshold, specify appropriate values for the following threshold fields:

- **Type**—Specify high, low, relativeChange, absoluteChange, rearmingAbsoluteChange.
- **Datasource**—Specify a name for the datasource.

- Datasource type—Specify a datasource type from the list.
- Datasource label—Specify a type from the list.
- Value—Use depends on the type of threshold.
- Re-arm— Specify the name of a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
- Trigger—Specify the number of times the threshold must be exceeded in a row before the threshold is triggered.



NOTE: A trigger is not used for relativeChange thresholds.

- Description—(Optional) A description used to identify the purpose of the threshold.
 - Triggered UEI— A custom UEI to send into the events system when the threshold is triggered. If a UEI is not specified, it defaults to the standard thresholds UEIs in the format *uei.opennms.org/<category>/<name>*.
 - Re-armed UEI—A custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
5. Select **Save** to create the threshold in Junos Space Network Management Platform.
 6. (Optional) To configure a resource filter for a threshold:
 - a. Configure a filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold. An OR operator specifies that if the resource matches any of the filters, the threshold is processed. An AND operator specifies that the threshold is processed only when a resource match all the filters.
 - b. Specify a field name for the filter the filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.
 - c. Specify the mathematical expression with data source names that is evaluated and compared to the threshold values.
 - d. Select the **Add** action to add the filter to a threshold.

To create an expression-based threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

The Edit group page appears.

3. Select **Create New Expression-based Threshold**

The Edit expression threshold page appears.

4. To configure the threshold, specify appropriate values for the following expression threshold fields:
 - Type—Specify high, low, relativeChange, absoluteChange, rearmingAbsoluteChange.
 - Expression—Specify a mathematical expression that includes the datasource names which are evaluated and compared to the threshold values.
 - Datasource type—Specify a datasource type from the list.
 - Datasource label—Specify a type from the list.
 - Value—Use depends on the type of threshold.
 - Re-arm— Specify the name of a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
 - Trigger—Specify the number of times the threshold must be exceeded in a row before the threshold is triggered.



NOTE: A trigger is not used for relativeChange thresholds.

- Description—(Optional) A description used to identify the purpose of the threshold.
- Triggered UEI— A custom UEI to send into the events system when the threshold is triggered. If a UEI is not specified, it defaults to the standard thresholds UEIs in the format `uei.opennms.org/<category>/<name>`.
- Re-armed UEI—a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.

5. Select **Save** to create the expression threshold in Junos Space Network Management Platform.
6. (Optional) To configure a resource filter for an expression threshold:
 - a. Configure a filter operator to define the logical function to apply for the expression threshold filter to determine whether or not to apply the expression threshold. An OR operator specifies that if the resource matches any of the filters, the expression threshold is processed. An AND operator specifies that the expression threshold is processed only when a resource match all the filters.
 - b. Specify a field name for the filter to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.
 - c. Specify the mathematical expression with data source names that are evaluated and compared to the threshold values.
 - d. Select the **Add** action to add the filter to an expression threshold.

Modifying Thresholds

To modify an existing threshold in a threshold group:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

The Threshold Configuration page appears and lists the threshold groups that are configured on the system.
2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

The Edit group page appears.
3. To modify an existing threshold, select the **Edit** option that appears to the right of the threshold you want to update.

The Edit Threshold page appears and displays the threshold fields.
4. Modify the threshold fields you want to update.

5. Click **Save** to update the threshold.
6. (Optional) To add a resource filter for the threshold:
 - a. Specify a filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold. An OR operator specifies that if the resource matches any of the filters, the threshold is processed. An AND operator specifies that the threshold is processed only when a resource match all the filters.
 - b. Specify a field name for the filter to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.
 - c. Specify the mathematical expression with data source names that are evaluated and compared to the threshold values.
 - d. Select the **Add** action to add the filter to the threshold.

Deleting Thresholds

To delete a threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.
The Threshold Configuration page appears and lists the threshold groups that are configured on the system.
2. To delete a threshold from a threshold group, select **Edit** next to the threshold group.
The Edit group page appears.
3. To delete an existing threshold, select **Delete**.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)

Selecting and Sending an Event to the Network Management System

To select and send an event:

1. Select **Network Monitoring > Admin > Send Event**.
The Send Event to OpenNMS page appears.
2. From the Events field, select an event from the list.
3. To define the event and the network monitoring destination, specify appropriate values for the following fields:
 - Node ID field—Select a device node from the list. The Node ID specifies the device in the event sent to the network monitoring system.
 - Source Hostname—Specify the hostname of the source from which the event is sent.
 - Interface field—Select the interface address to which the event is sent.

- Service field—Specify the name of the service that will receive the event.
 - Parameters—Click the **Add additional parameters** link to specify the name and value of each additional parameter you want to add.
 - Description field—Provide a description for the event.
 - Severity field—Select a severity level for the event.
 - Operator instructions—Include instructions that the operator might need to respond to the event notification.
4. Click **Send Event** to send the event to the system.

Configuring Notifications

- [Configuring Event Notifications on page 416](#)
- [Configure Destination Paths on page 418](#)
- [Configure Path Outages on page 419](#)

Configuring Event Notifications

You can configure an event to send a notification whenever that event is triggered. You can add, edit, and delete event notifications.

To add a notification to an event:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click **Add New Event Notification**.
3. Select the event UEI that will trigger the notification.
4. Click **Next**.
5. Build the rule that determines whether to send a notification for this event, based on the interface and service information specified in the event.
6. You can validate the rule results or skip the rule results validation:
 - To validate the rule results:
 - a. Click **Validate rule results**.
 - b. Click **Next**.
 - c. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - d. Click **Finish**.
 - To skip the rule results:
 - a. Click **Skip results validation**.

- b. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
- c. Click **Finish**.

To edit an existing event notification:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click the **Edit** button that is located to the left of the event notification you want to modify.
3. Select the event UEI that will trigger the notification.
4. Click **Next**.
5. Build the rule that determines whether to send a notification for this event, based on the interface and service information specified in the event.
6. (Optional) Click **Reset Address and Services** if you want to clear the changes that you have entered.
7. You can validate the rule results or skip the rule results validation:
 - To validate the rule results:
 - a. Click **Validate rule results**.
 - b. Click **Next**.
 - c. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - d. Click **Finish**.
 - To skip the rule results:
 - a. Click **Skip results validation**.
 - b. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - c. Click **Finish**.

To delete an existing event notification:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click the **Delete** button that is located to the left of the event notification you want to modify.
3. Click **Ok** in the delete notification confirmation dialog box to delete the notification.

Configure Destination Paths

You can configure a destination path that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. A destination path defines a reusable list of contacts that you include in an event configuration.

To create a new destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Click the **New Path** button.
3. Specify appropriate values for the following fields:
 - Name field—Specify a name for the destination path.
 - Initial Delay—From the list, select the number of seconds to wait before sending notifications to users or groups.
 - Initial targets—Select the users and groups to whom the event notification will be sent.
4. Click the **Add Escalation** button to specify users and groups to whom event notification will be sent.
5. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.
6. Click **Next**.
7. Click **Finish** when you have finished editing the destination path.

To modify an existing destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Under Existing Paths, select the existing destination path that you want to modify.
3. Click **Edit**.
4. You can make changes to any of the following fields:
 - Initial Delay—From the list, select the number of seconds to wait before sending notifications to users or groups.
 - Initial targets—Add users and groups to whom the event notification should be sent and remove users and groups to whom the event should not be sent.
5. Click the **Add Escalation** button to specify users and groups to whom event notification will be sent.
6. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.

7. Click **Next**.
8. Click **Finish** when you have finished modifying the destination path.

To delete a destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Under Existing Paths, select the existing destination path that you want to delete.
3. Click **Delete**.
4. Click **Ok** to confirm that you want to delete the selected destination path.

Configure Path Outages

You can configure a path outage that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. A destination path defines a reusable list of contacts that you include in an event configuration.

To create a new path outage:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Path Outage**.
2. Click the **New Path** button.
3. Specify appropriate values for the following fields:
 - Critical Path—Enter the critical path IP address.
 - Critical Path Service—From the list, select the ICMP protocol.
 - Initial targets—Select the users and groups to whom the event notification will be sent.
4. Build the rule that determines which nodes are subject to this critical path.
5. Select the **Show matching node list** check box to show the list of nodes that match.
6. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.
7. Click **Validate rule results** to validate the rule.
8. Click **Finish** when you have finished configuring the path outage.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)

Configuring Scheduled Outages

You can configure scheduled outages to suspend notifications, polling, thresholding and data collection (or any combination of these) for any interface/node for any length of time.

To create a scheduled outage:

1. Select **Network Monitoring > Admin > Scheduled Outages**.
2. Specify a name for the scheduled outage.
3. Click **Add new outage** to create the scheduled outage.
4. Build the rule that determines which nodes are subject to this critical path.
5. Specify appropriate values for the following fields:
 - Node Labels—From the list, select the node labels to add.
 - Interfaces—From the list, select the interfaces to add.
 - Outage type—From the list, select daily, weekly, monthly, or (time) specific.
 - Time—Specify one or more days and times for the outage.
6. Specify that the outage applies to one or more of the following categories:
 - Notifications
 - Status polling
 - Threshold checking
 - Data collection

Compiling SNMP MIBs

- [Uploading MIBs on page 420](#)
- [Compiling MIBs on page 421](#)
- [Viewing MIBs on page 421](#)
- [Deleting MIBs on page 421](#)
- [Clearing MIB Console Logs on page 422](#)
- [Generating Event Configuration on page 422](#)
- [Generating a Data Collection Configuration on page 423](#)

Uploading MIBs

To upload a MIB file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.
3. Click **Upload MIB**.
4. Browse and upload the MIB file from the appropriate location where the MIB file is stored.

The MIB file you have uploaded is displayed in the pending node of the MIB tree. You can now view and compile this MIB file.



NOTE: The filename must be the same as the MIB being processed.

Compiling MIBs

Before you compile a MIB file, ensure that you have uploaded the MIB file. The MIB file should be displayed in the pending node of the MIB tree for you to be able to compile the MIB file.

To compile a MIB file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.
3. From the pending node of MIB tree, right click the MIB file you want to compile and select **Compile MIB**.

You can view the results of the MIB compilation in the MIB Console section of Admin page. If the MIB file is compiled successfully, you will receive a log entry “MIB parsed successfully”. If the MIB file cannot be compiled, you will receive an error message.

If a MIB file is compiled successfully, the MIB file will be moved from the pending node to the compiled node in the MIB tree.

Viewing MIBs

You can view MIB files in the compiled state or in the pending state.

To view a MIB file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.
3. Right click the MIB file you want to view and select **View MIB**.

The View MIB pop-up window displays the MIB file. Use the scroll bar to view the contents of the MIB file.

Deleting MIBs

You can delete MIB files in the compiled state or in the pending state.

To delete a MIB file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. Right-click the MIB file you want to delete and select **Delete MIB**.
4. Click **Yes**.

Clearing MIB Console Logs

MIB console displays the logs related to MIB file upload and MIB file compilation.

To clear the MIB console logs:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.
3. Click **Clear Log** in the MIB console section.

Generating Event Configuration

You can generate event configuration from traps after you have compiled the MIB files.

To generate an event configuration:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.
3. From the compiled node in the MIB tree, right-click a MIB file and select **Generate Events**.
4. In the Generate Events pop-up window, click **Continue**.

You can edit the UEI base if needed. The Events window now displays the events that are currently part of the MIB file. You can choose to save this events XML file as is, edit this events XML file, or add new events to this file.

5. To save the events file as is, click **Save Events File**.
6. To add new events:
 - a. Click **Add Event**.
Enter the new event details.
 - b. In the Event UEI field, enter a unique event identifier.
 - c. In the Event Label field, enter a label for the new event.
 - d. In the Description field, enter a description for the new event.
 - e. In the Log Message field, enter a log message for the new event.
 - f. From the Destination drop-down menu, select an appropriate option.
 - g. From the Severity drop-down menu, select an appropriate option.
 - h. In the Reduction Key field, enter the appropriate text.

- i. In the Clear Key field, enter the appropriate text.
 - j. From the Alarm Type drop-down menu, select an appropriate option.
 - k. In the Operator Instructions field, enter instructions for the operator if required.
 - l. Click **Add** next to the Mask Elements table to add new element names and element values.
 - m. Click **Add** next to the Mask Varbinds table to add new varbind numbers and varbind values.
 - n. Click **Add** next to the Varbind Decodes table to add new parameter IDs and decode values.
 - o. Click **Save**.
 - p. Click **Yes**.
7. To edit the current events XML file:
 - a. Select the event you want to edit.
 - b. Scroll down to the bottom of the window and select **Edit**.

You can now edit all the parameters of this event.
 8. After you have added new events or modified the events, click **Save Events File**.



NOTE: Once an event file is saved, reference gets added to eventconf.xml and an event configuration reload operation is performed.

Generating a Data Collection Configuration

You can generate a data collection configuration for performance metrics after you have compiled the MIB files.

To generate a data collection configuration:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.
3. From the compiled node in the MIB tree, right-click a MIB file and select **Generate Data Collection**.

The Data Collection window is displayed. You can save the Data collection XML file as is or add new resource types, MIB groups, and system definitions to this data collection XML. You can also modify the existing resource types, MIB groups, and system definitions before saving the data collection XML.

4. In the Data Collection Group Name field, modify the group name if required.
5. To save the data collection XML as is, click **Save Data Collection File**.
6. To add a new resource type to the data collection XML:

- a. Select the Resource Types column in the Data Collection window.
 - b. Click **Add Resource Type**.
Enter the resource type details.
 - c. In the Resource Type Name field, enter a name for the resource.
 - d. In the Resource Type Label field, enter a label for the resource.
 - e. In the Resource Label field, enter the appropriate text.
 - f. From the Class Name drop-down menu, select the appropriate class name for storage strategy.
 - g. Click **Add** next to the Storage Strategy table to add new parameters.
 - h. From the Class Name drop-down menu, select the appropriate class name for persist selector strategy.
 - i. Click **Add** next to the Persist Selector Strategy table to add new parameters.
 - j. Click **Save**.
7. To edit an existing resource type in the data collection XML:
 - a. Select the Resource Types column in the Data Collection window.
 - b. Select the resource type you want to edit.
 - c. Scroll down to the bottom of the window and select **Edit**.
You can now edit all the parameters of this resource type.
8. To add a new MIB group to the data collection XML:
 - a. Select the MIB Groups column in the Data Collection window.
 - b. Click **Add Group**.
Enter the MIB group details.
 - c. In the Group Name field, enter a name for the MIB group.
 - d. From the ifType Filter drop-down menu, select the appropriate option.
 - e. Click **Add** next to the MIB Objects table to add the OID, instance, alias, and type for the MIB objects.
 - f. Click **Save**.
9. To edit an existing MIB group in the data collection XML:
 - a. Select the MIB Groups column in the Data Collection window.
 - b. Select the MIB group you want to edit.
 - c. Scroll down to the bottom of the window and select **Edit**.
You can now edit all the parameters of this MIB group.
10. To add a new system definition to the data collection XML:

- a. Select the System Definitions column in the Data Collection window.
- b. Click **System Definition**.
Enter the system definition details.
- c. In the Group Name field, enter a name for the system definition.
- d. Select the appropriate buttons next to the System OID/Mask field.
- e. Select the MIB group you want to associate this system definition to, and click **Add Group**.

The MIB group is displayed in the MIB Groups table.

- f. Click **Save**.
11. To edit an existing system definition in the data collection XML:
 - a. Select the System Definitions column in the Data Collection window.
 - b. Select the system definition you want to edit.
 - c. Scroll down to the bottom of the window and select **Edit**.

You can now edit all the parameters of this system definition.



NOTE: Update the `datacollection-config.xml` to include the group created into an SNMP collection when you have generated a data collection.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)

Managing Events Configuration Files

- [Adding New Events Configuration Files on page 425](#)
- [Deleting Events Configuration Files on page 426](#)
- [Modifying Events Configuration Files on page 426](#)

Adding New Events Configuration Files

To add a new events configuration file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **Manage Events Configuration** in the Operations section of the Admin page.
3. Click **Add New Events File**.
The New Events Configuration pop-up window is displayed.
4. In the Events File Name field, enter a name for the events configuration file.
5. Click **Continue** to add the events configurations file.

Deleting Events Configuration Files

To delete an events configuration file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **Manage Events Configuration** in the Operations section of the Admin page.
3. From the Select Events Configuration File drop-down menu, select the events configuration file you want to remove.
4. Click **Remove Selected Events File**.
5. Click **Yes**.

Modifying Events Configuration Files

You can edit the events in the events configuration XML file or add new events to this file.

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **Manage Events Configuration** in the Operations section of the Admin page.
3. From the Select Events Configuration File drop-down menu, select the events configuration file you want to modify.
4. To add new events to this events configuration file:
 - a. Click **Add Event**.
Enter the new event details.
 - b. In the Event UEI field, enter a unique event identifier.
 - c. In the Event Label field, enter a label for the new event.
 - d. In the Description field, enter a description for the new event.
 - e. In the Log Message field, enter a log message for the new event.
 - f. From the Destination drop-down menu, select an appropriate option.
 - g. From the Severity drop-down menu, select an appropriate option.
 - h. In the Reduction Key field, enter appropriate text.
 - i. In the Clear Key field, enter appropriate text.
 - j. From the Alarm Type drop-down menu, select an appropriate option.
 - k. In the Operator Instructions field, enter instructions for the operator if required.
 - l. Click **Add** next to the Mask Elements table to add new element names and element values.

- m. Click **Add** next to the Mask Varbinds table to add new varbind numbers and varbind values.
- n. Click **Add** next to the Varbind Decodes table to add new parameter IDs and decode values.
- o. Click **Save**.
5. To edit the current events configuration file:
 - a. Select the event you want to edit.
 - b. Scroll down to the bottom of the window and select **Edit**.
 You can now edit all the parameters of this event.
6. After you have added new events or modified the existing events, click **Save Events File**.
7. Click **Yes**.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)

Managing SNMP Collections

- [Add a New SNMP Collection on page 427](#)
- [Modify an SNMP Collection on page 428](#)

Add a New SNMP Collection

To add a new SNMP collection:

1. Select **Network Management Platform > Network Monitoring > Admin**.
 The Admin page is displayed.
2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.
3. Select the **SNMP Collections** tab.
4. Click **Add SNMP Collection**.
5. In the SNMP Collection Name field, enter a name for the SNMP collection.
6. From the SNMP Storage Flag drop-down menu, select an appropriate value.
7. Click **Add** next to the RRA list table and add consolidation function, XFF, steps, and rows for RRD.
8. Click **Add** next to the Include Collections table and add the include types and values.
9. Click **Save**.

Modify an SNMP Collection

To modify an SNMP collection:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.
3. Select the **SNMP Collections** tab.
4. Click **Refresh SNMP Collection**.
5. Select the appropriate SNMP collection name.
6. Scroll down to the bottom of the window and click **Edit**.
You can now edit all the parameters of this SNMP collection.
7. Click **Save**.

Related Documentation

- [Network Monitoring Workspace Overview on page 365](#)

Managing Data Collection Groups

- [Adding New Data Collection Files on page 428](#)
- [Deleting Data Collection Files on page 429](#)
- [Modifying Data Collection Files on page 429](#)

Adding New Data Collection Files

To add a new data collection file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.
3. Select the **Data Collection Groups** tab.
4. Click **Add New Data Collection File**.
The New Data Collection Group pop-up window is displayed.
5. In the Group Name field, enter a name for data collection group.
6. Click **Continue** to add and configure the data collection file.

Deleting Data Collection Files

To delete a data collection file:

1. Select **Network Management Platform > Network Monitoring > Admin**.
the Admin page is displayed.
2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.
3. Select the **Data Collection Groups** tab.
4. From the Select Data Collection Group File drop-down menu, select the data collection file you want to remove.
5. Click **Remove Selected Data Collection File**.
6. Click **Yes**.

Modifying Data Collection Files

You can edit the resource types, MIB groups, or system definitions in the data collection file or add new resource types, MIB groups, or system definitions to this file.

1. Select **Network Management Platform > Network Monitoring > Admin**.
The Admin page is displayed.
2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.
3. Select the **Data Collection Groups** tab.
4. From the Select Data Collection Group File drop-down menu, select the data collection file you want to modify.
5. To add a new resource type to the data collection file:
 - a. Select the Resource Types column in the Data Collection window.
 - b. Click **Add Resource Type**.
Enter the resource type details.
 - c. In the Resource Type Name field, enter a name for the resource.
 - d. In the Resource Type Label field, enter a label for the resource.
 - e. In the Resource Label field, enter the appropriate text.
 - f. From the Class Name drop-down menu, select the appropriate class name for the storage strategy.
 - g. Click **Add** next to the Storage Strategy table to add new parameters.
 - h. From the Class Name drop-down menu, select the appropriate class name for the persist selector strategy.

- i. Click **Add** next to the Persist Selector Strategy table to add new parameters.
 - j. Click **Save**.
6. To edit an existing resource type in the data collection file:
 - a. Select the **Resource Types** column in the Data Collection window.
 - b. Select the resource type you want to edit.
 - c. Scroll down to the bottom of the window and select **Edit**.

You can now edit all the parameters of this resource type.
7. To add a new MIB group to the data collection file:
 - a. Select the MIB Groups column in the Data Collection window.
 - b. Click **Add Group**.

Enter the MIB group details.
 - c. In the Group Name field, enter a name for the MIB group.
 - d. From the ifType Filter drop-down menu, select the appropriate option.
 - e. Click **Add** next to the MIB Objects table to add the OID, instance, alias, and type for the MIB objects.
 - f. Click **Save**.
8. To edit an existing MIB group in the data collection file:
 - a. Select the MIB Groups column in the Data Collection window.
 - b. Select the MIB group you want to edit.
 - c. Scroll down to the bottom of the window and select **Edit**.

You can now edit all the parameters of this MIB group.
9. To add a new system definition to the data collection file:
 - a. Select the System Definitions column in the Data Collection window.
 - b. Click **System Definition**.

Enter the system definition details.
 - c. In the Group Name field, enter a name for the system definition.
 - d. Select the appropriate radio buttons next to the System OID/Mask field.
 - e. Select the MIB group you want to associate this system definition to, and click **Add Group**.

The MIB group is now displayed in the MIB Groups table.
 - f. Click **Save**.
10. To edit an existing system definition in the data collection file:
 - a. Select the **System Definitions** column in the Data Collection window.
 - b. Select the system definition you want to edit.

- c. Scroll down to the bottom of the window and select **Edit**.

You can now edit all the parameters of this system definition.

11. When you have made the necessary changes, select **Save Data Collection File**.

**Related
Documentation**

- [Network Monitoring Workspace Overview on page 365](#)

Managing Devices

- [Managing Surveillance Categories on page 433](#)

Managing Surveillance Categories

You can specify the devices for which SNMP data collection is controlled in different surveillance categories. Surveillance categories determine whether the data for the device is collected for performance management monitoring. You can modify, delete, and add surveillance categories.

- [Modifying Surveillance Categories on page 433](#)
- [Deleting Surveillance Categories on page 433](#)
- [Adding Surveillance Categories on page 433](#)

Modifying Surveillance Categories

To modify a surveillance category:

1. Select **Network Monitoring > Admin > Manage Surveillance Categories**.
2. Click the icon in the Edit column in the same row as the category.

The Edit Surveillance Category page appears.

3. To add devices to the surveillance category, select the device from the Available nodes list and click **Add**.
4. To remove devices from the surveillance category, select the device from the Nodes on category list and click **Remove**.

Deleting Surveillance Categories

To remove a surveillance category, click the icon in the Delete column in the same row as the category.

Adding Surveillance Categories

To add a surveillance category:

1. Select **Network Monitoring > Admin > Manage Surveillance Categories**.
2. Enter the name in the box and click **Add New Category**.

The name appears on the Surveillance Categories page.

3. Click the name in the Category column, and click **Edit category** on the Surveillance Category page.
4. To add devices to the surveillance category, select the device from the Available nodes list and click **Add**.
5. To remove devices from the surveillance category, select the device from the Nodes on category list and click **Remove**.

**Related
Documentation**

- [Turning SNMP Data Collection Off and On on page 372](#)
- [Network Monitoring Workspace Overview on page 365](#)

Configuring Alarm Notifications

- [Alarm Notification Configuration Overview on page 435](#)
- [Configuring Alarm Notification on page 438](#)

Alarm Notification Configuration Overview

By default, the alarms generated by managed devices in the Junos Space platform are sent to the network monitoring functionality. To enable alarm notification for supported Junos Space applications, you can configure the **alarmNotificationConf.xml** file to specify the alarm notifications that designated Junos Space applications should receive. The applications will receive only those alarms that you configure in the **alarmNotificationConf.xml** file and that match the specified filter criteria.

You can configure basic and advanced filters so that any alarms that match the configured filtering conditions are forwarded to the designated applications.

- [Basic Filtering on page 435](#)
- [Guidelines for Configuring Alarm Notifications on page 436](#)
- [Advanced Filtering on page 436](#)

Basic Filtering

You configure a basic filter to filter alarms based on the Unique Event Identifier (UEI), device family, and severity. At minimum, you must configure a UEI filter. Filtering by device family, severity, or both, is optional.

To configure a basic filter for alarm notification, at minimum, you must configure the following notification tags in the **alarmNotificationConf.xml** file, which must reside in the **/opt/opennms/etc/alarm-notification** directory:

- Notification name
- UEI of the alarm to be notified
- The script to be executed for the configured UEI

You can also configure the following tags in the **alarmNotificationConf.xml** file:

- Severity—Supported severity values are Indeterminate, Cleared, Normal, Warning, Minor, Major, and Critical

When configuring an alarm for notification, a notification is sent for the corresponding Clear Alarm. A notification is also sent after clearing an alarm from the user interface. To forward notification for Clear alarms and user interface (UI) , you must configure **Severity = Normal, Cleared**.

- Device Family—Supported device family is present in the **devicefamily.properties** in the **/opt/opennms/etc/alarm-notification**.



NOTE: If the Sysoid for the device is unknown, the **DevicesWithNoSysoid** filter is matched.

Guidelines for Configuring Alarm Notifications

Use the following guidelines when configuring alarm notifications:

- To send notification when an alarm is cleared from the UI, you must include **event uei.opennms.org/vacuumd/juniper/alarmCleared** in the **eventconf.xml** file.
- The event entry is present in **/opt/opennms/etc/examples/alarm-notification/eventconf.xml**. This entry should be added to **/opt/opennms/etc/eventconf.xml**.



NOTE: Do not copy and paste the entire **/opt/opennms/etc/examples/alarm-notification/eventconf.xml** file. If the event entry is not already present, append the event entry to the existing **eventconf.xml** file.

- The tags listed in the **/opt/opennms/etc/examples/alarm-notification/vacuumd-configuration.xml** file should be added to the **/opt/opennms/etc/vacuumd-configuration.xml** file, if not already present.
- Alarm notification dampening is performed based on the alarm counter. The **notification_threshold** attribute is added for this purpose. The default value is 5, which specifies that the first alarm is notified, then the sixth alarm, and so on.

Advanced Filtering

To provide more in-depth filtering, you must configure a drool (DRL) file. With advanced filtering, the applications receive only those alarms that match all the advanced filtering conditions. The name of the drool file and notification name mentioned in the **alarmNotificationConf.xml** file should match, and for each notification, there must be a drool file whose name matches the notification name. Each drool file that you configure must be added to the **/opt/opennms/etc/alarm-notification/drools** directory. You can view a sample drool file from the **/opt/opennms/etc/examples/alarm-notification/drools** directory. You can view a sample **alarmNotification.xml** file from the **/opt/opennms/etc/examples/alarm-notification** directory.



NOTE: Care should be taken when writing the rule. For each rule that satisfies the condition, a corresponding script is invoked. For better performance, do not configure multiple rules for the same UEI.

You can create advanced filters based on any combination of the following fields:

- alarmacktime
- alarmackuser
- alarmid
- alarmtype
- applicationdn
- clearkey
- counter
- description
- dpname
- eventparms
- eventuei
- firsteventtime
- ifindex
- ifname
- ipaddr
- lasteventtime
- logmsg
- ossprimarykey
- operinstruct
- reductionkey
- serviced
- severity
- suppressedtime
- suppresseduntil
- suppresseduser
- tticketid
- tticketstate
- uiclear

- [x733Alarmtype](#)
- [x733Probablecause](#)

**Related
Documentation**

- [Configuring Alarm Notification on page 438](#)

Configuring Alarm Notification

By default, the alarms generated by managed devices in the Junos Space platform are sent to the network monitoring functionality. To enable alarm notification for supported Junos Space applications, you can configure alarm notification files for basic filtering to specify the alarm notifications that designated Junos Space applications should receive.

- [Configuring a Basic Filter for Alarm Notification on page 438](#)
- [Activating Alarm Notification Configuration Files for Basic Filtering on page 439](#)
- [Reloading a Filter Configuration to Apply Filter Configuration Changes on page 440](#)

Configuring a Basic Filter for Alarm Notification

The following steps show how to configure a basic filter based on unique event identifier (UEI), severity, and device family. When the alarm criteria specified in the XML file are matched, the alarm XML is passed as an argument to the invoked script.

To configure a basic filter for alarm notification:

1. Configure the destination for the notification in the script, for example, **Sample_App_Script.sh**. The script specifies how the alarm notifications are sent to the application.

```
curl -v -u super:juniper123 -X POST -H "Content-Type:application/xml" -d "$xml"
"http://localhost:8080/SampleApplication/services/Alarms"
```



NOTE: In the preceding example, the curl command is used to post the script, but the configuration of the script can vary based on the requirements of the application.

You can access sample configuration scripts from the `/opt/opennms/etc/examples/alarm-notification/scripts` directory. However, all active scripts must be present in the `/opt/opennms/etc/alarm-notification/scripts` directory.

2. In the **alarmNotificationConf.xml** configuration file:

- a. Enable the alarm notification feature:

```
<notification name="SampleAppNotification" enable="true">
```

- b. Configure the number of seconds to wait for the script to execute before timing out:

```
<script timeout_in_seconds="45">
```



NOTE: If you do not configure the `timeout_in_seconds` attribute, the default time out for the script invoked is 60 seconds. In this case, the shell exit status will be '143' and error handling will be considered in the same way as other error exit status. If the script continues to execute after the timeout value for the script, alarm notification will not wait for the script status. During this time, processing of other alarms will not be blocked.

- c. Specify the name of the script that will be invoked:

```
<scriptname>Sample_App_Script.sh</scriptname>
```

The configured script must be present in the `/opt/opennms/etc/alarm-notification/scripts` directory.

- d. Enable error handling, and configure the number of notification retry attempts and interval (in seconds) between retry attempts, if the initial attempt to send the notification fails:

```
<errorhandling enable="true">
  <retry_interval_inseconds>3</retry_interval_inseconds>
  <number_of_retries>2</number_of_retries>
</errorhandling>
```



NOTE: The script exit status should be '0' if there are no errors. For other exit status values, the script will be invoked again if error handling is enabled.

- e. Configure the UEI of the alarms which will require notification:

```
<uies>
  <uei name="uei.opennms.org/generic/traps/SNMP_Link_Down"
notification_threshold="5"
  <filter devicefamily="JSeries" severity="Minor,Normal"/>
  <filter devicefamily="DevicesWithNoSysoid" severity="Minor,Normal"/>
  <uei/>
</uies>
```

Activating Alarm Notification Configuration Files for Basic Filtering

After configuring the alarm notification files for basic filtering, you must add the files to the Junos Space application to activate the alarm notification configuration:

1. Log in from the Junos Space system console.

The Junos Space Appliance Settings menu displays.

2. From the Junos Space Appliance Settings menu, enter 7 (or enter 8 from the Junos Space Virtual Appliance) to run the shell.

3. (Optional): To view the sample configuration files for alarm notification:
 - Navigate to the `/opt/opennms/etc/examples/alarm-notification` directory to view sample files for `alarmNotificationConf.xml`, `eventconf.xml`, and `vacuumd-configuration.xml`.
 - Navigate to the `/opt/opennms/etc/examples/alarm-notification/scripts` directory to view the `CBU_App_Script.sh` and `NA_App_Script.sh` sample scripts.
4. To activate configuration files for alarm notification, perform the following steps:
 - a. Add your configured `alarmNotificationConf.xml` file to the `/opt/opennms/etc/alarm-notification` directory.
 - b. Add your configured `eventconf.xml` and `vacuumd-configuration.xml` files to the `/opt/opennms/etc` directory.
 - c. Add your configured script file to the to the `/opt/opennms/etc/alarm-notification/scripts` directory.

Reloading a Filter Configuration to Apply Filter Configuration Changes

After making any changes to a filter, you can reload the configuration by sending a "reloadDaemonConfig" event, for example:

```
/opt/opennms/bin/send-event.pl -p 'daemonName Alarmd.AlarmNorthbouncer'  
uei.opennms.org/internal/reloadDaemonConfig
```

You do not need to restart the server to apply the configuration changes listed in previous steps. However, to send the event, go to `/opt/opennms/bin ./send-event.pl -p 'daemonName Alarmd.AlarmNorthbouncer' uei.opennms.org/internal/reloadDaemonConfig`.

This event will reload the following files:

- `alarmNotificationConf.xml`
- `devicefamily.properties`
- Drool (.drl) files

Related Documentation

- [Alarm Notification Configuration Overview on page 435](#)

PART 8

Configuration Files

- [Manage Configuration Files on page 443](#)
- [Backup Config Files on page 453](#)

CHAPTER 47

Manage Configuration Files

- [Managing Configuration Files Overview on page 444](#)
- [User Privileges in Configuration File Management on page 445](#)
- [Viewing Configuration File Statistics and Inventory on page 446](#)
- [Deleting Configuration Files on page 446](#)
- [Restoring Configuration Files on page 447](#)
- [Comparing Configuration Files on page 448](#)
- [Editing Configuration Files on page 450](#)
- [Exporting Configuration Files on page 452](#)

Managing Configuration Files Overview

Centralized configuration file management enables you to maintain copies of your device configuration files within Junos Space Network Management Platform, storing multiple versions of any configuration file. It therefore provides for device configuration recovery. It also facilitates maintaining configuration consistency across multiple devices.



NOTE: Because each commit command on a device creates a new version on that device, backup copies may not be kept long. No more than 49 copies can be stored on a device. Junos Space Network Management Platform provides backups with longer life-cycles.

Version management for configuration files in Junos Space Network Management Platform is therefore independent from the configuration file versioning on devices.

The configuration file management work space handles three types of configuration file:

- Running configuration—The configuration file currently in effect on the device. The running configuration file is labeled Version 0.
- Candidate configuration—The new, not yet committed, configuration file that will become the running configuration.
- Backup configuration—The configuration file for recovery or rollback purposes. A backup configuration file is created by a commit command and the oldest backup (version 49) is deleted. The most recent backup configuration file is labeled Version 1.

A potential workflow for an individual file or device in this work space could be:

- Backup device and thus bring device's running configuration under Junos Space Network Management Platform management
- Edit a copy of the backup configuration to create a candidate configuration
- Verify edits by comparing the initial backup version of the configuration file with the edited version
- Restore the candidate configuration to the device
- Export the initial backup to a zip file
- Delete the initial backup from Junos Space Network Management Platform.

Stored configurations can be viewed by double-clicking the item on the Manage Configuration Files page.

A dialog box appears, displaying the file in a non-editable format. You can select the version you want to view from the **Version** list.

The status bar near the bottom of the dialog box shows the current page number, the total number of pages in the file, and provides paging controls and a Refresh button. Below that is the Comments area.

To perform an action on a configuration file, either select one and select an action from the Actions menu, or right-click a configuration file and select an action from the right mouse-click menu. You can perform the following actions:

- [Deleting Configuration Files on page 446](#)
- [Restoring Configuration Files on page 447](#)
- [Comparing Configuration Files on page 448](#)
- [Editing Configuration Files on page 450](#)
- [Exporting Configuration Files on page 452](#)

Backing up configuration files counts as a task; see [“Backing Up Configuration Files” on page 454](#).

User Privileges in Configuration File Management

In Junos Space Network Management Platform, there is a predefined role for configuration file management: **Configuration File Manager**. That predefined role enables the users to which it has been assigned the permission to:

- Backup Configuration Files
- Delete Configuration Files
- Restore Configuration Files
- Compare Configuration Files
- Export Configuration Files

If you want to restrict the Configuration File Manager's permissions to anything less than the full set listed above, you can create a role and then assign the permissions specifically for each list item. For creating a user-defined role, [“Creating a User-Defined Role” on page 505](#).

Related Documentation

- [Role-Based Access Control Overview on page 479](#)
- [Managing Configuration Files Overview on page 444](#)

Viewing Configuration File Statistics and Inventory

The Configuration Files statistics page, which is directly under the Configuration Files workspace, displays two bar charts, showing:

- The Configuration file count by device family
- The most frequently revised configuration files.

In both cases, mouse over the graphic to display the contents in a tooltip.

All configuration files in Junos Space Network Management Platform are displayed on the **Config Files Management** inventory landing page. You can view stored configurations by double-clicking an entry in the table view.

The following information appears for each configuration file:

- Host Name
- IP Address
- Platform
- Serial Number of Device
- Software Version

Related Documentation

- [Backing Up Configuration Files on page 454](#)
- [Managing Configuration Files Overview on page 444](#)
- [Tags Overview on page 687](#)

Deleting Configuration Files

This topic gives the procedure for deleting device configuration files from Junos Space Network Management Platform.

To delete a configuration file, do the following:

1. Select **Configuration Files > Config Files Management**.

The Config Files Management page displays all the configuration files saved in Junos Space Network Management Platform.

2. Select the check box of a configuration file and click the **Delete Config Files** icon.

A message appears, asking you to confirm deletion.

3. Click **Delete**.

The Config Files Management page reappears, displaying any remaining configuration files.

- Related Documentation**
- [Managing Configuration Files Overview on page 444](#)
 - [Restoring Configuration Files on page 447](#)
 - [Comparing Configuration Files on page 448](#)
 - [Editing Configuration Files on page 450](#)
 - [Exporting Configuration Files on page 452](#)

Restoring Configuration Files

Restoring a configuration file means either merging the contents of a configuration file on Junos Space Network Management Platform with the existing configuration on the device, or overriding the device's running configuration with a candidate configuration (a configuration file edited in the Config Files workspace) or a backup from Junos Space Network Management Platform.

A restore action generates an audit log entry.

To restore a device configuration file from Junos Space Network Management Platform to a device:

1. Select **Configuration Files > Config Files Management**.
2. Select the device whose configuration you want to restore. (To restore all of them, select the check box in the column header next to **Device Name**.)
3. Select **Restore Config File** from the Actions menu.
The **Restore Config File(s)** dialog box appears, displaying the name of the selected file, the name of the device, the version which is to be restored to the device, and the type of restore. By default, the latest version will be merged.
4. Select the appropriate version from the drop-down list that appears when you click next to the version number displayed in the **ConfigFile Versions** column.
5. Select the appropriate type of restore from the drop-down list that appears when you click next to the term displayed in the **Type** column.
6. You can either restore immediately or schedule the restoration for a later time.
 - To restore Immediately, click **Restore**.
 - To schedule the restore at a later time:
 - a. Select the check box next to the **Schedule at a Later Time** label or click the arrow next to the **Schedule at a Later Time** label to display the corresponding fields.
 - b. Select a date from the field on the left, and a time from the field on the right. The time zone displays to the right of the time field. The time zone is set on and for the Junos Space server.
 - c. Click **Restore**.

The **Restore Configuration Files** dialog box appears, announcing the successful scheduling of the restoration, and presenting a link to the job ID so that you can view details.

A successful restore action will be indicated by the word **Success** in the status column of the Job Manager. If a device cannot be reached, it will be skipped over, and the job status will indicate failure.

7. Click **OK** to dismiss the dialog box.
8. (Optional) Verify your work either by double-clicking the configuration file name on the Manage Configuration Files page, or by doing another backup, then comparing versions (see [“Comparing Configuration Files” on page 448](#)).

**Related
Documentation**

- [Managing Configuration Files Overview on page 444](#)
- [Deleting Configuration Files on page 446](#)
- [Comparing Configuration Files on page 448](#)
- [Editing Configuration Files on page 450](#)
- [Exporting Configuration Files on page 452](#)
- [Backing Up Configuration Files on page 454](#)
- [Viewing Audit Logs on page 532](#)

Comparing Configuration Files

View entire device configurations side by side to compare them, see the total number of diffs run, the date and time of the last commit, and the number of changes made.

Using this feature does not generate an audit log entry.

You can compare the following:

- The configuration file of one device to the configuration file of another device. By default, the latest versions are compared.
- Two versions of the same configuration file. By default, the latest version and the previous version are compared.
- An earlier version of the configuration file of one device with a later version of the configuration file of another device.

Any choices other than those listed above will result in a dimmed (unavailable) menu.

To compare device configuration files:

1. Select **Configuration Files > Config Files Management**.

The Config Files Management page appears, displaying all the configuration files managed by Junos Space Network Management Platform.

2. Select the configuration file you want to compare.

3. Select **Compare Config File Versions** from the Actions menu.

The Compare Config Files page appears.

4. For the source, select a configuration file from the Source config file list and a version from the Version list.
5. For the target, select a configuration file from the Target config file list and a version from the Version list.
6. Click **Compare**.

The Compare Config Files dialog box displays the two configuration files side by side, with their file names and their versions in a dark gray bar underneath the legend at the top of the page. The legend references the following:

- Total diffs—Black text indicates content common to both files.
- Source—Content in the file on the left that is not contained in the file on the right.
- Target—Content in the file on the right that is not contained in the file on the left.
- Changed—Hot pink text indicates content unique to its respective file.

The status bar shows the current page number and the total number of pages. It also provides controls for moving from page to page and for refreshing the display.

The date and time of the last commit is shown in hot pink.



NOTE: When you compare files, each configuration parameter in one file or version is set side by side with the same parameter in the other. Therefore, you might see multiple pages of configuration for a single parameter in one file, whereas the same parameter in the other file might be only a couple of lines.

7. (Optional) To locate differences in configuration, click **Prev Diff** or **Next Diff**.
8. To finish viewing a comparison, click **Close** at the bottom of the page.

Related Documentation

- [Backing Up Configuration Files on page 454](#)
- [Managing Configuration Files Overview on page 444](#)
- [Deleting Configuration Files on page 446](#)
- [Restoring Configuration Files on page 447](#)
- [Editing Configuration Files on page 450](#)
- [Exporting Configuration Files on page 452](#)

Editing Configuration Files

This action enables a very advanced user to edit the configuration file of the selected device in a text editor. It is therefore very different from the Device Configuration Editor available as an Action in the Devices work-space (See [“Modifying Device Configuration Overview” on page 53](#)).



NOTE:

The Edit Config Files action in the Config Files work-space has no validation and no sanity check. To get those features, use the Edit Device Configuration action in the Devices work-space.

Editing a configuration file generates an audit log entry (see [“Viewing Audit Logs” on page 532](#)); however, unlike configuration files edited in the Devices work-space, files edited in the Config Files work-space are not saved as change requests, instead, they are saved as versions.

To edit a configuration file using the Edit Config File action in the Config Files work-space:

1. Select **Configuration Files > Config Files Management** and select the device whose configuration you want to edit.

If no configuration files are displayed on the page, you must first back up the discovered devices (see [“Backing Up Configuration Files” on page 454](#)).

2. Select **Modify Config File** from the Actions menu.

The Edit Config File page appears. It displays the name of the file you selected, the time at which the file was created, the version, and the contents.

3. Select a version to use as a baseline from the **Version** list.

A version can be either a backup of a device configuration, or an edited copy of that initial backup. For an explanation of versioning in this context, see [“Backing Up Configuration Files” on page 454](#).

The selected version appears in the text editor. Note that there are usually both vertical and horizontal scroll bars, and that a configuration usually has multiple pages. The status bar at the bottom displays the page you are on and the total number of pages. It also holds paging controls and a Refresh icon.

For ease of orientation, the pagination of the configuration file remains the same, even if you add or remove large quantities of text. The parameters that were on page 5 when you began editing are still on page 5 when you finish.

4. (Optional) To find a specific parameter, go through the file page by page. The browser's Search function does not work in the text editor.
5. Enter your changes, using the Copy/Paste function if required.



NOTE: Do not click **Modify** until you have finished editing.

6. (Optional) List the changes you have made (or anything else) in the Comments field. You cannot create a comment unless you have made changes. It is advisable to enter something in this field to distinguish the current version from a backup taken from the device itself.

7. When finished making all changes, click **Modify**

The Manage Configuration Files page reappears, displaying the edited configuration file still selected.

8. (Optional) Verify your work by double-clicking the device from the Manage Configuration Files page.

A dialog box appears, displaying the file in a non-editable format. You can select the version from the drop-down list. By default, the edited version appears.

Here again, the pagination, Comments area, and controls are the same as they are in the text editor you used to make your changes.

Alternatively, you could compare versions of the file (see [“Comparing Configuration Files” on page 448](#)).

To deploy the edited configuration file, you must use the Restore action (see [“Restoring Configuration Files” on page 447](#)).

Related Documentation

- [Managing Configuration Files Overview on page 444](#)
- [Deleting Configuration Files on page 446](#)
- [Restoring Configuration Files on page 447](#)
- [Comparing Configuration Files on page 448](#)
- [Exporting Configuration Files on page 452](#)
- [Backing Up Configuration Files on page 454](#)
- [Viewing Audit Logs on page 532](#)

Exporting Configuration Files

The Export action enables you to save one or more configuration files to a zip file on your local computer.



NOTE: Your browser security settings must be set to allow downloads. If the browser interrupts the download with a warning and then tries to restart the download by refreshing, the export will be aborted, and the zip file removed.

Exporting a configuration file generates an audit log entry.

To export a configuration file to a zip file,

1. Select **Configuration Files > Config Files Management** and select one or more configuration files.
2. Select **Compare Config File Versions** from the Actions menu.

The Export Config File(s) dialog box opens, displaying the name of the file, the device name, and the configuration file versions stored. By default, the latest version is selected.

3. Select the appropriate version from the drop-down list that appears when you click next to the version number displayed in the Versions column.
4. Click **Export**.

The Generating ZIP archive dialog box appears, displaying a progress bar showing when the zip file is ready for downloading, at which point, the Opening deviceConfigFiles.zip dialog box opens.

5. Save the zip file to your computer before closing the progress bar or the OpeningdeviceConfigFiles.zip dialog box, because the generated zip file is removed from the server immediately after the download is complete, or when either of these two dialog box is closed. Refreshing or exiting the browser will also remove the zip file from the server.

Related Documentation

- [Managing Configuration Files Overview on page 444](#)
- [Deleting Configuration Files on page 446](#)
- [Restoring Configuration Files on page 447](#)
- [Comparing Configuration Files on page 448](#)
- [Editing Configuration Files on page 450](#)
- [Backing Up Configuration Files on page 454](#)
- [Viewing Audit Logs on page 532](#)

CHAPTER 48

Backup Config Files

- [Backing Up Configuration Files on page 454](#)

Backing Up Configuration Files

Backing up a configuration file in the Config Files work-space means importing the configuration file from the device, and storing it in Junos Space Network Management Platform.

Backing up your device configurations is therefore the prerequisite for configuration file management (see [“Managing Configuration Files Overview” on page 444](#)).

Only devices that have been previously discovered can have their configuration files backed up. The backup function skips over any devices that cannot be reached. In the Job Manager, under Job Status, a skipped-over configuration file backup shows up as Failed.

The backup function checks for differences before creating a new version of a configuration file. If no changes are detected, the device is skipped over. However, its status is shown as Success.



NOTE: The backup function checks for differences between the configuration on the device and the backup configuration stored in Junos Space Network Management Platform. Therefore, even if no change to a device's configuration has been committed, if you edit its configuration file in Junos Space Network Management Platform and then make a backup, a new version is created. The first backup is version 1, the edited configuration file is version 2, and the second backup is version 3.

A configuration file backup generates an audit log entry.



NOTE: In the case of an SRX series device with LSYS, backup configuration is supported only for the root device.

To back up your device configuration files to Junos Space Network Management Platform:

1. Select **Configuration Files > Config Files Management** and select the Backup Config Files icon.

The **Backup Config Files** page appears, displaying all the devices managed by Junos Space Network Management Platform, with the following information:

- Host Name
- IP Address
- Platform
- Serial Number
- Software Version

Because the table displays one device (record) per row, a single page might not be sufficient to list all your devices. However, if you have tagged your devices, you can achieve a more manageable display by selecting devices according to their tag.

The left side of the status bar at the bottom of the dialog box shows which page you are looking at and the total number of pages of records. It also provides controls for navigating from page to page and refreshing them. The right side of the status bar indicates the number of records currently displayed and the total number of records.

2. Select the devices whose configurations you want to back up by using either of two selection modes—manual or tag-based. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option is selected and the full list of devices is displayed.

3. To select devices manually:

- a. Click the **Select by Device** option and select the device(s) whose configurations you want to back up.

The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.

- b. To back up all the devices, select the check box in the column header next to Host Name.

To select devices based on tags:

- a. Click the **Select by Tags** option.

The Select by tags list is activated.

- b. Click the arrow on the **Select by Tags** list.

A list of tags defined on devices in the Junos Space system appears.

- The list displays two subcategories of tags—Public and Private.
 - A check box is next to each tag name.
 - You can select one or more check boxes to select one or more tags.
 - As soon as you start to enter text in the **Select by Tags** field left of the **OK** button, if a match is found, a suggestion is made, and you can select it.
- c. Select the check boxes next to the displayed tag names as desired, or search for specific tags by clicking the magnifying glass Search icon. When you have made your selection, click **OK** to save the selected tags.
 - The total number of devices associated with the selected tags appears in the Select Devices status bar above the options.
 - The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.
 - Below this lower status bar appears the **Preview of Selections** list, displaying a table showing the devices selected and for each, the information described in step 1.

4. To back up the selected config files, choose one of the following options:

- Immediately
- Schedule for a Later Time—This results in one backup per device.
 - a. Select the check box next to **Schedule at a Later Time** or click the arrow next to it to display the corresponding fields.
 - b. Select a date from the field on the left, and select a time from the field on the right. The time zone is displayed to the right of the time field. The time zone is set on and for the Junos Space server.

- Repeat—Results in scheduled repetition, that is, multiple backups per device
 - a. Select the check box next to the Repeat label or click the arrow next to the Repeat label to display the corresponding fields.
 - b. Choose Minutes, Hours, Days, Weeks or Years from the list.
 - c. To set the frequency of the repetition, enter the appropriate whole number in the upper field.
 - d. (Optional) Set the End Time:

Select the check box next to the End Time label or click the arrow next to the End Time label to display the corresponding fields.
 - e. Select a date from the field on the left, and select a time from the field on the right. The time zone is displayed to the right of the time field. The time zone is set on and for the Junos Space server.

5. Click **Backup**.

The Backup Configuration Files dialog box appears, announcing that Junos Space Network Management Platform has successfully scheduled backup of the selected configuration files, and giving you a job ID link to view details.

6. Click **OK**.

The Manage Configuration Files page reappears, displaying the backup files. The page shows the following headers:

- Config File Name—This is the device name with .conf file ending.
- Device Name
- Latest Revision—This is always 1.
- Creation Date
- Last Updated Date

Click any header to reveal the down arrow, which you can click to sort, add, or delete column headers. You can also filter. For instructions on filtering, see [“Filtering Inventory Pages” on page 27](#).

Related Documentation

- [Managing Configuration Files Overview on page 444](#)
- [Deleting Configuration Files on page 446](#)
- [Restoring Configuration Files on page 447](#)
- [Comparing Configuration Files on page 448](#)
- [Editing Configuration Files on page 450](#)
- [Exporting Configuration Files on page 452](#)
- [Tagging an Object on page 695](#).
- [Viewing Audit Logs on page 532](#)

PART 9

Jobs

- [Overview on page 461](#)
- [Manage Jobs on page 465](#)
- [Archive Jobs on page 473](#)

Overview

- [Jobs Overview on page 461](#)

Jobs Overview

The Jobs workspace lets you monitor the status of all jobs that have been run in all Junos Space applications. A job is a user-initiated action that is performed on a Junos Space Network Management Platform object, such as a device, service, or customer. All scheduled jobs can be monitored.

Typical jobs in Junos Space Network Management Platform include device discovery, deploying services, prestaging devices, and performing functional and configuration audits. Jobs can be scheduled to occur immediately or in the future. For all jobs scheduled in Junos Space Network Management Platform, you can view job status from the **Jobs** workspace. Junos Space Network Management Platform maintains a history of job status for all scheduled jobs. When a job is scheduled from a workspace, Junos Space Network Management Platform assigns a job ID that serves to identify the job (along with the job type) in the Manage Jobs inventory page.

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

- View status of all scheduled, running, canceled, and completed jobs
- Retrieve details about the execution of a specific job
- View statistics about average execution times for jobs, types of jobs that are run, and success rate
- Cancel a scheduled job or in-progress job (when the job has stalled and is preventing other jobs from starting)
- Archive old jobs and purge them from the Junos Space Network Management Platform database

Junos Space Network Management Platform supports the following job types:



NOTE: The job types listed here may not represent the job types you are able to manage in your Junos Space Network Management Platform software release. Job types are subject to change based on the installed applications in your Junos Space Network Management Platform software release.

Table 71: Junos Space Job Types Per Application

Junos Space Application	Supported Job Types
Network Management Platform	Add Node
	Discover Network Elements
	Update Device
	Delete Device
	Resync Network Element
	Role Assignment
	Audit Log Archive and Purge
Network Activate	Deploy Service
	Prestage Device
	Role Assignment
	Service Deployment
	Service Decommission
	Functional Audit
	Configuration Audit
Service Now	Install AI-Scripts
	Uninstall AI-Scripts
Ethernet Design	Provision Device Profile
	Provision Port Profile
Security Design	Provisioning Security
	Policy Provisioning IPSec VPN
	Importing Address/Domain in Security Topology
QoS Design	Discover Domain
	Create QoS Profile

**Related
Documentation**

- [Viewing Scheduled Jobs on page 466](#)
- [Viewing Statistics for Scheduled Jobs on page 469](#)
- [Canceling a Job on page 470](#)
- [Viewing Database Backup Job Recurrence on page 471](#)
- [Archiving and Purging Jobs on page 473](#)

CHAPTER 50

Manage Jobs

- [Viewing Your Jobs on page 465](#)
- [Viewing Scheduled Jobs on page 466](#)
- [Viewing Statistics for Scheduled Jobs on page 469](#)
- [Canceling a Job on page 470](#)
- [Viewing Job Recurrence on page 471](#)
- [Retrying a Job on Failed Devices on page 472](#)

Viewing Your Jobs

You can view all your completed, in-progress, and scheduled jobs in Junos Space Network Management Platform. You can quickly access summary and detailed information about all your jobs, from any work space and from any task you are currently performing. You can also clear jobs from your list when jobs are no longer of interest to you.

To view the jobs that you have initiated:

1. In the banner of the Junos Space user interface, click the My Jobs icon.

The My Jobs report appears. The My Jobs report displays your 25 most recent jobs.

The jobs displayed in the My Jobs report provide information about the status of the job, percentage completion of the job, the name of the job, and the job ID. The date and time represents the date and time when the job failed (in case the job failed) and the date and time when the job succeeded (in case the job succeeded).

2. To view jobs details, click **Manage My Jobs**.

The Job Management page displays a listing of all jobs that you initiated.

You can also click a job in the My Jobs report to view the job on the Job Management page. Clicking the job ID filters the Job Management page to display only that job.

3. To remove jobs from the My Jobs report:

- To remove a job, click the Clear job icon that appears to the right of the job.



NOTE: Clearing a job from the My Jobs report does not affect the job itself, but only updates the My Jobs view.

- Related Documentation**
- [Viewing Statistics for Scheduled Jobs on page 469](#)
 - [Canceling a Job on page 470](#)
 - [Jobs Overview on page 461](#)

Viewing Scheduled Jobs

The Manage Jobs inventory page displays all jobs that have been scheduled to run or have run from each Junos Space application.

- [The View on page 466](#)
- [Viewing Job Types on page 466](#)
- [Viewing Job Status Indicators on page 466](#)
- [Viewing Job Details, Status, and Results on page 467](#)
- [Performing Manage Jobs Commands on page 468](#)

The View

Scheduled and completed jobs appear as rows in the Manage Jobs inventory table. By default, jobs appear sorted by scheduled start time. You can sort on other criteria.

To display the Manage Jobs table:

- Select **Jobs > Job Management**.
The Job Management table appears.

Viewing Job Types

The job type appears as a column in the Job Management table. Job types tell you what tasks or operations have been performed throughout Junos Space applications. Each Junos Space application supports certain job types. You can search for a particular job type. You can also sort by job type in tabular view. For more information about how to manipulate inventory page data, see [“Junos Space User Interface Overview” on page 9](#).

Viewing Job Status Indicators

Each job has a job status indicator. [Table 72 on page 466](#) defines these indicators.

Table 72: Job Icon Status Indicators






Job Status Indicator	Description
	The job was completed successfully.
	The job failed.

Table 72: Job Icon Status Indicators (*continued*)

	The job was canceled by a user.
	The job is scheduled.
	The job is in progress. You can only cancel jobs that are in progress from the Actions menu.

Viewing Job Details, Status, and Results

The Job Management table shows most of what you need to know about each job. You can get more details about a particular job from the Job Details window. To see these details, double-click that job's row in the Job Management table.

[Table 73 on page 467](#) defines job information. The job information that appears in the Job Management table and in the Job Details window varies with the type of job. This table defines all the possible entries.

Table 73: Job Details and Columns in the Manage Jobs Table

Field	Description
ID	The numerical ID of the job.
Name	For most jobs, the name is the job type with the job ID appended. However, for some jobs the job name is supplied by the user as part of the workflow.
Percent	The percentage of the job that has been completed.
State	The state of job execution: <ul style="list-style-type: none"> • SUCCESS—Job completed successfully. • FAILURE—Job failed and was terminated. • IN PROGRESS—Job is in progress. • CANCELED—Job was canceled by a user.
Job Type	The supported job types. Job types depend on the installed Junos Space applications.
Summary	The operations executed for the job.
Scheduled Start Time	The start time you have specified for this job.
User	The user's login name.
Recurrence	The scheduled recurrence.
Retry Group ID	Job ID of the original job.
Previous Retry	Job ID of the previous job.

Table 73: Job Details and Columns in the Manage Jobs Table (*continued*)

Job Details (depending on job type):	
IP Address	The address of the device on which the operation is performed.
Hostname	The name of the device on which the operation is performed.
Status	The job status: SUCCESS, FAILURE, IN PROGRESS, or CANCELED.
Description	Explanatory detail about a failure.
Actual Start Time	The time when Junos Space Network Management Platform begins execution of the job. In most cases, actual start time should be the same as the scheduled start time.
End Time	The time when the job was completed or was terminated, if job execution failed.
Backup Date	The date on which you backed up the database.
Comment	An optional note that describes or otherwise identifies the backup operation.
Machine	The name of the Junos Space server from which database backup occurred.
File Path	The pathname to the database backup file.

Performing Manage Jobs Commands

You can perform the following commands from the Manage Jobs Actions menu:

- Cancel Job—Stop a scheduled job. See [“Canceling a Job” on page 470](#).
- View Recurrence—Displays the View Job Recurrence dialog box, from which you can view the recurring database job start date and time, recurrence interval, end date and time, and job ID for each occurrence. See [“Viewing Database Backup Job Recurrence” on page 471](#).
- Return to Application—Returns to the application page from which this job was initiated (if you have the correct permissions to do so).
- Tag It—Apply a tag to a job to segregate, filter, and categorize jobs. See [“Tagging an Object” on page 695](#).
- View Tags—View tags applied to a job. See [“Viewing Tags for a Managed Object” on page 696](#).
- Untag It—Remove a tag from a job. See [“Untagging Objects” on page 697](#).

Related Documentation

- [Viewing Statistics for Scheduled Jobs on page 469](#)
- [Jobs Overview on page 461](#)
- [Canceling a Job on page 470](#)

Viewing Statistics for Scheduled Jobs

The Jobs workspace statistics page displays the following graphical data:

- Job Types pie chart
- State of Jobs Run pie chart
- Average Execution Time per Completed Job bar chart

This topic includes the following tasks:

- [Viewing the Types of Jobs That Are Run on page 469](#)
- [Viewing the State of Jobs That Have Run on page 469](#)
- [Viewing Average Execution Times for Jobs on page 470](#)

Viewing the Types of Jobs That Are Run

The Job Types pie chart displays the percentage of all Junos Space Network Management Platform jobs of a particular type that are run. Each slice in the pie chart represents a job type and the percentage of time that job type was run. The job type legend appears to the right, identifying the job type titles according to colors. Scroll down the list to see all the job types. The numbers of jobs in the job types legend represent jobs run in all Junos Space applications. Mousing over a slice in the pie chart displays the job type title and the number of jobs that have run.

- To display details of only a specific job type, click that job type in the Job Types pie chart.
A filtered list of these jobs appears in tabular form on the Job Management page. For more information about the Job Management page, see [“Viewing Scheduled Jobs” on page 466](#).
- To return to the Job Management page, select **Job Management** in the breadcrumbs at the top of the Manage Jobs page.

Viewing the State of Jobs That Have Run

The State of Jobs Run pie chart graphically displays the percentages of jobs that have succeeded or failed. Mouse over the pie chart to see the numbers of jobs in each slice.

- To display details of only those jobs that have succeeded or those that have failed, click the appropriate slice in the State of Jobs Run pie chart.
The filtered jobs appear displayed in tabular form on the Job Management page. For more information about the Job Management page, see [“Viewing Scheduled Jobs” on page 466](#).
- To return to the Job Management page, select **Job Management** in the breadcrumbs at the top of the Manage Jobs page.

Viewing Average Execution Times for Jobs

Each bar in the Average Execution Time per Completed Job bar chart represents a job type and the average execution time in seconds. If there is room on the display, the name of the job type appears at the bottom of each bar.

- To display details of only jobs of a given type, click a bar in the Average Execution Time per Completed Job bar chart.
The filtered jobs appear displayed in tabular form on the Job Management page. For more information about the Job Management page, see [“Viewing Scheduled Jobs” on page 466](#).
- To return to the Job Management page, select **Job Management** in the breadcrumbs at the top of the Manage Jobs page.

Related Documentation

- [Viewing Scheduled Jobs on page 466](#)
- [Jobs Overview on page 461](#)
- [Junos Space User Interface Overview on page 9](#)
- [Archiving and Purging Jobs on page 473](#)

Canceling a Job

You can cancel jobs from the Job Management workspace using the Cancel job task. You can cancel the jobs that are already scheduled for execution. You can also cancel jobs that are not completed for a long time or jobs that are hindering the execution of other jobs in the queue.

If you are a user who is assigned the privileges of a Job Administrator, you can cancel jobs scheduled by any user. If you are a user who is assigned the privileges of a Job User, you can only cancel jobs that are scheduled by you. If you are assigned a role that does not allow you to cancel any job, you cannot cancel any job in the Jobs workspace.

If you are a user administrator creating a custom role, you can assign the privileges of a Job Administrator or a Job User to the new user.



NOTE: If Junos Space Network Management Platform determines that the job operation is non-interruptible, the job runs to completion; otherwise the job is canceled.



NOTE: Junos Space Network Management Platform does not cleanup canceled jobs.

You can cancel other users' jobs if you are assigned a role that has the privileges of a Job Administrator. If you are not assigned a role that has the privileges of a Job Administrator,

you will not be able to cancel other users' jobs. All jobs except the jobs you triggered will be greyed out.

To cancel a job:

1. Select **Jobs > Job Management**.

The Job Management inventory page appears.

2. Select the job that you want to cancel.

3. Select **Cancel Job** from the Actions menu.

If a job is in a state that you cannot cancel, The Cancel Job command is disabled in the Actions menu.

When the Cancel Job operation completes, the inventory page displays the Job State as CANCELED.

**Related
Documentation**

- [Viewing Statistics for Scheduled Jobs on page 469](#)
- [Jobs Overview on page 461](#)
- [Viewing Scheduled Jobs on page 466](#)
- [Junos Space User Interface Overview on page 9](#)
- [Viewing Your Jobs on page 465](#)

Viewing Job Recurrence

You can view information about when a job recurs. For example, you can examine the recurrence of a database backup job.

To view job recurrence information:

1. Select **Jobs > Job Management**.

The Job Management page appears.

2. Select a recurring job and select **View Recurrence** from the Actions menu.

The View Job Recurrence dialog box displays the selected job start date and time, recurrence interval, and end date and time.

3. (Optional) Click the **Job ID** link to view all recurrences of the schedule.

4. Click **OK** on the View Job Recurrence dialog box to return to the Job Management page.

**Related
Documentation**

- [Backing Up the Junos Space Network Management Platform Database on page 605](#)
- [Viewing Scheduled Jobs on page 466](#)
- [Viewing Audit Logs on page 532](#)

Retrying a Job on Failed Devices

To rerun a job that was not successful:

1. In **Jobs > Job Management**, select the job you want to retry.

The **Retry Job - Devices Selection** window appears. The status bar at the bottom of the table has page controls so that you can page through to verify your selection.

2. To select the devices on which to run the job, either:

- Select devices from the **Select Applicable Devices** table, showing the following for each device:
 - Name
 - IP address
 - Job status—Failed/Failure, Success, or Cancelled
 - Description—Explains the nature of the failure

or

- If you want to run the job on all the devices listed over multiple pages, choose **Select All Devices Across Pages**.

The check boxes in the table showing the device listings are unavailable.

3. (Optional) To view the devices on which the job cannot be rerun, click **View Inapplicable Devices**.

The **View Inapplicable Devices** window appears with a table listing all the inapplicable devices. You can view the same information for each device as the **Select Applicable Devices** table.

To close the window, click **Cancel**.

4. (Optional) To run this job at a different time, select the **Schedule at a later time** check box.

Select the date and time to run it from the date and time drop down lists that appear.

5. Click **Run**.

The **Resynchronization Information** window appears.

6. To view details, click the job ID. To close the window, click **OK**.

The **Manage Jobs** page reappears, showing your job rerun.

- Related Documentation**
- [Jobs Overview on page 461](#)
 - [Viewing Your Jobs on page 465](#)

Archive Jobs

- [Archiving and Purging Jobs on page 473](#)

Archiving and Purging Jobs

As Junos Space Network Management Platform runs over time, the number of job entries in the database increases, which affects system query performance. In most cases, a job's results become obsolete and unused after a few hours. These jobs can be archived as a CSV file to either the local server or a remote server, and then they can be purged to improve performance. Junos Space Network Management Platform will from time to time remind you to archive old jobs.

You can archive completed jobs (successful or not) that occurred before any date and time up to the present. You must be an administrator to use this function.

Archive files, audit logs, and related files are stored in the default location `/var/lib/mysql/archive`, or in a directory that you specify. The default filename for an archive is `JunosSpaceJobsArchive_date_time_id.zip`, where *date* specifies the year, month, and day, in the format `yyyy-mm-dd`; *time* specifies hours, minutes, and seconds, in the format `hh-mm-ss`; and *id* is a six-character number in the format `xx-xx-xx` that uniquely identifies each job archive file.

This topic includes the following tasks:

- [Archiving Jobs to a Local Server and Purging the Database on page 473](#)
- [Archiving Jobs to a Remote Server and Purging the Database on page 474](#)

Archiving Jobs to a Local Server and Purging the Database

You can archive jobs to the local server. The local server is the server that functions as the active node in the Junos Space fabric.

To archive Junos Space Network Management Platform jobs to the local server and then purge them from the database:

1. Select **Jobs > Job Management** and select the Archive/Purge Jobs icon. The Archive/Purge Jobs dialog box appears.
2. In the Archive Jobs Before field, select a date and time to specify the date up to which all jobs are to be archived and then purged from the Junos Space Network Management Platform database. You can specify only a date and time in the past.



NOTE: If you do not specify a date and time in the Archive Jobs Before field, Junos Space Network Management Platform archives and then purges from the database all jobs up to the time that you initiated the operation.

3. In the Archive Mode field, select **local** from the list.
4. To schedule the Archive/Purge operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the Archive/Purge operation when you complete this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the Archive/Purge operation.



NOTE: The selected time in the scheduler maps to Junos Space server time but uses the local time zone of the client computer.

5. Click **Submit**.

The Jobs Archive and Purge confirmation dialog box displays the archive filename and the location where it will be saved.
6. Click **Continue** to archive and purge the jobs.
7. To view job details for the operation, select the Job Id in the Job Information dialog box; otherwise, click **OK** to close the dialog box.

Archiving Jobs to a Remote Server and Purging the Database

You can archive jobs to remote network hosts or media. Junos Space Network Management Platform uses scp (secure copy) to copy the files in this case.

To archive jobs to a remote host and then purge them from the Junos Space Network Management Platform database:

1. Select **Jobs > Job Management** and select the Archive/Purge Jobs icon. The Archive/Purge Jobs dialog box appears.
2. In the Archive Jobs Before field, select a date and time to specify the date up to which all jobs are to be archived and then purged from the Junos Space Network Management Platform database. You can specify only a date and time in the past.



NOTE: If you do not specify a date and time in the Archive Jobs Before field, Junos Space Network Management Platform will archive and then purge from the database all jobs up to the time that you initiated the operation.

3. In the Archive Mode field, select **Remote** from the list.
4. Enter a valid username to access the remote host server.
5. Enter a valid password to access the remote host server.
6. Reenter the password you entered in the previous step.
7. Enter the IP address of the remote host server.
8. Enter a directory path on the remote host server for the archived log files.



NOTE: The directory path must already exist on the remote host server.

9. Schedule the archive and purge operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the Archive/Purge operation when you complete this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the Archive/Purge operation.



NOTE: The selected time in the scheduler maps to Junos Space server time but uses the local time zone of the client computer.

10. Click **Submit**.

The Jobs Archive and Purge dialog box displays the file location and the name of the remote server.

11. Click **Continue** to archive and purge the audit logs.

Junos Space Network Management Platform displays the Jobs Archive and Purge Job Information dialog box.

12. To view job details for the Archive/Purge operation, click the **Job Id** link.
13. Click **OK** to close the dialog box.

**Related
Documentation**

- [Jobs Overview on page 461](#)
- [Viewing Your Jobs on page 465](#)
- [Viewing Scheduled Jobs on page 466](#)
- [Viewing Database Backup Job Recurrence on page 471](#)

PART 10

Users

- [Manage Roles on page 479](#)
- [Manage User-Defined Roles on page 505](#)
- [Manage Users on page 509](#)
- [Manage Remote Profiles on page 525](#)
- [User Sessions on page 527](#)

CHAPTER 52

Manage Roles

- [Role-Based Access Control Overview on page 479](#)
- [Understanding How to Configure Users to Manage Objects in Junos Space on page 480](#)
- [Predefined Roles Overview on page 481](#)
- [Managing Roles Overview on page 502](#)
- [Managing Roles on page 503](#)

Role-Based Access Control Overview

Junos Space Network Management Platform supports authentication and authorization. A Junos Space super administrator or user administrator creates users and assigns roles (permissions) that allow users to access and manage the users, nodes, devices, configlets, scripts, services, and customers in Junos Space Network Management Platform.

To access and manage Junos Space Network Management Platform, a user must be assigned one or more roles, which are validated during authorization. The roles that an administrator assigns to a user control the workspace or workspaces the user can access and the tasks that can be performed on the objects that are managed within a workspace. A user with no role assignments cannot access any Junos Space Network Management Platform workspace and is unable to perform tasks.

Authentication

Through authentication, Junos Space Network Management Platform validates users based on password and other security services. Junos Space Network Management Platform supports both local and remote user authentication in different scenarios. For local authentication, each user password is saved in the Junos Space Network Management Platform database and is used to validate a user during login. Remote authentication by a RADIUS or TACACS+ server is supported. See [“Configuring a RADIUS Server for Authentication and Authorization” on page 673](#).

RBAC Enforcement

With role-based access control (RBAC) enforcement, a Junos Space super administrator or user administrator controls the workspaces a user can access, the system resources users can view and manage, and the tasks available to a user within a workspace. RBAC is enforced in the Junos Space user interface navigation hierarchy by workspace, task group, and task. A user can access only those portions of the navigation hierarchy that

are explicitly granted through access privileges. The following sections describe RBAC enforcement behavior at each level of the user interface navigation hierarchy.

Enforcement by Workspace

The Junos Space user interface provides a task-oriented environment in which a collection of related user tasks is organized by workspace. For example, the Users workspace defines the group of tasks related to managing users and roles. Tasks include creating, modifying, and deleting users, and assigning roles. Enforcement by workspace ensures that a user can view only those workspaces that contain the tasks that the user has permissions to execute. For example, a user who is assigned the device manager role, which grants access privileges to all tasks in the Devices workspace, can access only the Devices workspace. No other workspaces are visible to this user unless other roles are assigned to this user.

RBAC Enforcement Not Supported for Getting Started Page

RBAC enforcement is not enabled for the contents of the Getting Started page. Consequently, a user who does not have certain access privileges can still view the steps displayed in the Getting Started page. For example, a user without privileges to manage devices still sees the Discover Devices step. However, when the user clicks on the step, Junos Space Network Management Platform displays an error to indicate that the user might not have permission to access the workspace or tasks to which the step is linked.

Related Documentation

- [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)
- [Managing Permission Labels Overview on page 701](#)
- [Predefined Roles Overview on page 481](#)
- [Creating User Accounts on page 509](#)
- [Viewing User Statistics on page 524](#)
- [Viewing Users on page 516](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 673](#)

Understanding How to Configure Users to Manage Objects in Junos Space

Junos Space Network Management Platform is shipped with a super administrator privilege level that has full access to the Junos Space system. When you first log in to Junos Space as default super administrator, you can perform all tasks and access all Junos Space system resources. The super administrator can create new users and assign roles to those users to specify which workspaces and system resources users can access and manage, and which tasks users can perform within each workspace.

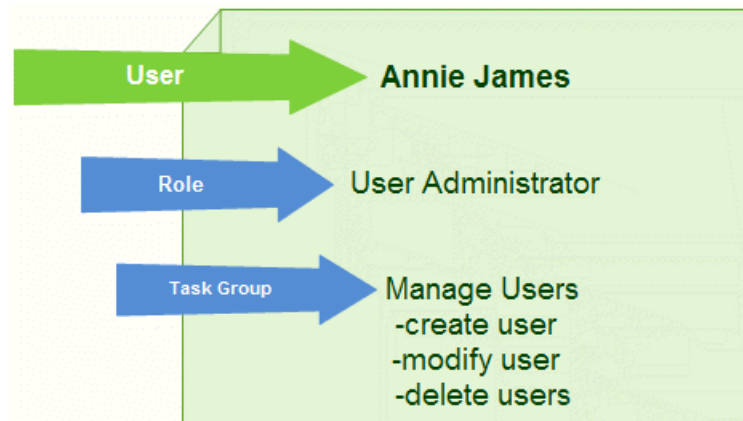
After you first set up Junos Space Network Management Platform, you can disable the default super administrator user ID, if necessary. However, before doing so, you should first create another user with super administrator privileges.

To access and manage Junos Space system resources, a user must be assigned at least one role. A *role* defines the tasks (create, modify, delete) that can be performed on the

objects (devices, users, roles, configlets, scripts, services, customers) that Junos Space Network Management Platform manages. For complete information on the predefined roles, see [“Predefined Roles Overview” on page 481](#).

Users receive permission to perform tasks only through the roles that they are assigned. In most cases, a single role assignment enables a user to view and to perform tasks on the objects within a workspace. For example, a user assigned the Device Manager role can discover devices, resynchronize devices, view the physical inventory and interfaces for devices, and delete managed devices. A user that is assigned the User Administrator role can create, modify, and delete other users in Junos Space, and assign and remove roles.

Typically a role contains one or more task groups. A *task group* provides a mechanism for grouping a set of related tasks that can be performed on a specific object. The following illustration shows the task group and associated tasks that are available to a user that is assigned the User Administrator role.



NOTE: You can assign multiple roles to a single user, and multiple users can be assigned the same role.

Related Documentation

- [Role-Based Access Control Overview on page 479](#)
- [Managing Permission Labels Overview on page 701](#)
- [Creating User Accounts on page 509](#)
- [Viewing Users on page 516](#)
- [Viewing User Statistics on page 524](#)

Predefined Roles Overview

Junos Space Network Management Platform provides predefined roles that you can assign to users to define administrative responsibilities and specify the management tasks that a user can perform within applications and workspaces.

To assign roles to other users in Junos Space Network Management Platform, a user must be a super administrator or user administrator.

Each predefined role defines a set of tasks for a single workspace, except the super administrator role, which defines all tasks for all workspaces. By default, Junos Space Network Management Platform provides Read privileges on all objects associated with the task groups defined in a predefined role.

Table 74 on page 482 shows the Junos Space Network Management Platform predefined roles and corresponding tasks available for installed Junos Space applications.



NOTE: The predefined roles that appear in the Junos Space Network Management Platform release that you are using depend on the Junos Space applications that you have installed. For the latest predefined roles, see **Network Management Platform > Users > User Accounts > Create User** or **Network Management Platform > Roles**.

Table 74: Predefined Roles for the Junos Space Network Management Platform

Predefined Role	Task Group and Tasks	Application > Workspace
Audit Log Administrator	<ul style="list-style-type: none"> Audit Logs <ul style="list-style-type: none"> Archive/Purge Logs Export Audit Logs 	Network Management Platform > Audit Logs
Configuration File Manager	<ul style="list-style-type: none"> Configuration Files <ul style="list-style-type: none"> Configuration Files Management <ul style="list-style-type: none"> Backup Config Files Delete Config File Restore Config File Compare Config File Versions Export Config File Modify Config File 	Network Management Platform > Config Files
Device Image Manager	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Adapter <ul style="list-style-type: none"> Add Adapter Upgrade Adapter Delete Adapter Images and Scripts <ul style="list-style-type: none"> Images <ul style="list-style-type: none"> Import Images View Deploy Results Modify Device Image Delete Device Images Stage Image on Device MD5 Validation Result Verify Checksum Deploy Device Image 	Network Management Platform > Devices Network Management Platform > Device Images and Scripts

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Images Read Only User	<ul style="list-style-type: none">• Images and Scripts<ul style="list-style-type: none">• Images• View Deploy Results	Network Management Platform > Device Images and Scripts

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Manager		Network Management Platform > Images and Scripts

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Device Discovery <ul style="list-style-type: none"> • Discover Targets • Specify Probes • Specify Credentials • Device Management <ul style="list-style-type: none"> • Delete Devices • Put in RMA State • Reactivate from RMA • Change Device Credentials • View Physical Inventory • Export Physical Inventory • Upload Authentication Key • Modify Device Configuration • Edit Device Configuration • View Change Requests • Manage Consolidated Config <ul style="list-style-type: none"> • Generate Consolidated Config • Prepare Consolidated Config • Validate on Device Consolidated Config • Approve Consolidated Config • Reject Consolidated Config • Deploy Consolidated Config • View/Assign Shared Objects • View Space Changes • Resolve Out-of-band Changes • View Config Change Log • View Physical Interfaces • View Logical Interfaces • View License Inventory • View Software Inventory • Launch Device WebUI • Create LSYS • View Alarms • View Performance Graphs • Resynchronize with Network • SSH to Device • Looking Glass • Upload Keys to Devices • Secure Console • Deployed Devices <ul style="list-style-type: none"> • Add Devices • Download Management CLIs • View Device Status • Delete 	

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> Unmanaged Devices Clone 	
Device Script Manager	<ul style="list-style-type: none"> Scripts <ul style="list-style-type: none"> Compare Script Versions Import Script View Execution Results Modify Script Delete Scripts Stage Scripts on Devices View Associated Devices Verify Scripts on Devices Verification Results Enable Scripts on Devices Disable Scripts on Devices Remove Scripts from Devices Execute Script on Devices Export Scripts Modify Scripts Type Script Bundles <ul style="list-style-type: none"> Create Script Bundles Modify Delete Stage on Devices View Device Association Enable Script Bundle on Devices Disable Script Bundle on Devices Execute on Devices 	
Device Script Read Only User	<ul style="list-style-type: none"> Device Images and Scripts <ul style="list-style-type: none"> Scripts <ul style="list-style-type: none"> Compare Script Versions View Execution Results View Associated Devices Export Scripts Script Bundles 	Network Management Platform > Images and Scripts

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
FMPM Manager	<ul style="list-style-type: none"> • Network Monitoring <ul style="list-style-type: none"> • Node List <ul style="list-style-type: none"> • Resync Nodes • Search • Outages • Dashboard • Events • Alarms • Notifications • Assets • Reports • Charts • Topology • Admin 	Network Management Platform > Network Monitoring

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Operation Manager		Network Management Platform > Devices Network Management Platform > Images and Scripts

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Devices <ul style="list-style-type: none"> • Device Adapter <ul style="list-style-type: none"> • Add Adapter • Upgrade Adapter • Delete Adapter • Images and Scripts <ul style="list-style-type: none"> • Images <ul style="list-style-type: none"> • Import Images • View Deploy Results • Modify Device Image • Delete Device Images • Stage Image on Device • MD5 Validation Result • Verify Checksum • Deploy Device Image • Scripts <ul style="list-style-type: none"> • Compare Script Versions • Import Script • View Execution Results • Modify Script • Delete Scripts • Stage Scripts on Devices • View Associated Devices • Verify Scripts on Devices • Verification Results • Enable Scripts on Devices • Disable Scripts on Devices • Remove Scripts from Devices • Execute Script on Devices • Export Scripts • Modify Scripts Type • Script Bundles <ul style="list-style-type: none"> • Create Script Bundle • Modify • View Device Association • Enable Script Bundle on Devices • Disable Script Bundle on Devices • Stage on Devices • Delete • Execute on Devices • Operations <ul style="list-style-type: none"> • Create Operation • Copy Operation • Modify Operation • Delete Operations 	

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Import Operations • Export Operations • Run Operation • View Operation Results 	
Job Administrator	<ul style="list-style-type: none"> • Job Management <ul style="list-style-type: none"> • Cancel My Job • Cancel Any Job • Archive/Purge Jobs • View Recurrence 	Network Management Platform > Job Management
Job User	<ul style="list-style-type: none"> • Job Management <ul style="list-style-type: none"> • Cancel My Job • View Recurrence 	Network Management Platform > Job Management
Permission Label Administrator	<ul style="list-style-type: none"> • Administration <ul style="list-style-type: none"> • Perm Labels <ul style="list-style-type: none"> • Rename Permission Label • Delete Permission Labels • Create Perm Label • Assign Permission Labels to Users • Remove Permission Labels from Users • Attach Permission Label to Objects • Detach Permission Label from Objects 	Network Management Platform > Administration
Super Administrator	Manage all Junos Space Network Management Platform task groups and tasks (See Network Management Platform > Users > User Accounts user interface for the current roles.)	Access all Junos Space Network Management Platform workspaces

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
System Administrator	<ul style="list-style-type: none"> Fabric <ul style="list-style-type: none"> Add Fabric Node Delete Fabric Node Space Node Settings SNMP Configuration System Snapshot Generate Key Backup and Restore <ul style="list-style-type: none"> Backup Delete Backup Restore Restore from Remote File Troubleshoot Space Applications <ul style="list-style-type: none"> Modify Application Settings Manage Services Add Application Uninstall Application Upgrade Application Upgrade Platform Licenses <ul style="list-style-type: none"> Import License Tags <ul style="list-style-type: none"> Create Tag Rename Tag Delete Tags Share Tag Perm Labels <ul style="list-style-type: none"> Create Perm Label Rename Permission Label Delete Permission Labels Assign Permission Labels to Users Remove Permission Labels from Users Attach Permission Label to Objects Detach Permission Label from Objects DMI Schemas <ul style="list-style-type: none"> Set Default Schema Report Missing Schemas Update Schema Manage Auth Servers Manage SMTP Servers 	Network Management Platform > Administration

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Tag Administrator	<ul style="list-style-type: none"> Tags <ul style="list-style-type: none"> Rename Tag Delete Tag Share Tag Create Tags 	Network Management Platform > Administration > Tags
Template Design Manager	<ul style="list-style-type: none"> Device Templates <ul style="list-style-type: none"> Definitions <ul style="list-style-type: none"> Create Template Definition Manage CSV Files Modify Template Definition Clone Template Definition Publish Template Definition Unpublish Template Definition Delete Template Definition Export Template Definition Import Template Definition 	Network Management Platform > Device Templates
Template Manager	<ul style="list-style-type: none"> Device Templates <ul style="list-style-type: none"> Create Template Modify Template Delete Template Deploy Template Audit Template Config Undeploy Template View Template Deployment Template Consolidated Configuration 	Network Management Platform > Device Templates

Table 74: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
User Administrator	<ul style="list-style-type: none"> • Users <ul style="list-style-type: none"> • User Accounts <ul style="list-style-type: none"> • Create User • Modify User • Clear Local Passwords • Delete Users • Disable Users • Enable Users • Roles <ul style="list-style-type: none"> • Create Role • Modify Role • Delete Role • Remote Profiles <ul style="list-style-type: none"> • Create Remote Profile • Modify Remote Profile • Delete Remote Profiles • User Sessions <ul style="list-style-type: none"> • Terminate User Session 	Network Management Platform > Users

[Table 75 on page 493](#) shows the Junos Space predefined roles for the Network Activate application.

Table 75: Predefined Roles for Network Activate Application

Predefined Role	Task Group and Tasks	Workspace
Service Designer	<ul style="list-style-type: none"> • Manage Service Definitions <ul style="list-style-type: none"> • Create Point-to-Point (P2P) Service Definition • Custom Service Definition • Create VPLS Service Definition • Publish Service Definition • Unpublish Service Definition 	Service Design

Table 75: Predefined Roles for Network Activate Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
Service Manager	<ul style="list-style-type: none"> • Manage Device Roles <ul style="list-style-type: none"> • Rules • Discovery Roles • Unassign NPE Role • Manage Device UNIs • Delete UNI • Add Device UNIs • Assign UNI • Assign Roles • Modify Loopback Address • Manage Device UNIs • Exclude from UNI Role • Exclude from NPE Role • Assign NPE Role 	Prestage Devices
Service Activator	<ul style="list-style-type: none"> • Manage Customers <ul style="list-style-type: none"> • Create Customer • Modify Customer • Delete Customers • Manage Service Orders <ul style="list-style-type: none"> • Create Point-to-Point (P2P) Service Order • Deploy Service Order • Delete Service Order • Create VPLS Service Order • Manage Services <ul style="list-style-type: none"> • Modify Service • Decommission Service • View Configuration Audit Results • Perform Configuration Audit • View Functional Audit Results • Perform Functional Audit • View Service Configuration 	Service Provisioning

Table 76 on page 495 shows the Junos Space predefined roles for the Service Insight application.

Table 76: Predefined Roles for Service Insight Application

Service Insight Administrator	<ul style="list-style-type: none"> Insight Central <ul style="list-style-type: none"> Exposure Analyzer <ul style="list-style-type: none"> Show Matching PBNs Generate EOL Reports EOL Reports <ul style="list-style-type: none"> Regenerate EOL Reports Export EOL Reports Delete Targeted PBNs <ul style="list-style-type: none"> Scan for Impact Flag to Users Email PBN to Users Assign Ownership Delete Notifications <ul style="list-style-type: none"> Create Notifications Edit Filters and Actions Copy Delete Enable/Disable 	Service Insight
Service Insight Read Only User	<ul style="list-style-type: none"> Insight Central <ul style="list-style-type: none"> Exposure Analyzer <ul style="list-style-type: none"> Show Matching PBNs EOL Reports <ul style="list-style-type: none"> Export EOL Reports Targeted PBNs <ul style="list-style-type: none"> Scan for Impact Notifications 	Service Insight

Table 76: Predefined Roles for Service Insight Application (*continued*)

Service Insight Unrestricted User	<ul style="list-style-type: none">• Insight Central<ul style="list-style-type: none">• Exposure Analyzer<ul style="list-style-type: none">• Show Matching PBNs• Generate EOL Reports• EOL Reports<ul style="list-style-type: none">• Regenerate EOL Reports• Export EOL Reports• Delete• Targeted PBNs<ul style="list-style-type: none">• Scan for Impact• Flag to Users• Email PBN to Users• Assign Ownership• Delete• Notifications<ul style="list-style-type: none">• Create Notifications• Edit Filters and Actions• Copy• Delete• Enable/Disable	Service Insight
--------------------------------------	---	-----------------

[Table 77 on page 497](#) shows the Junos Space predefined roles for the Service Now application.

Table 77: Predefined Roles for Service Now Application

Predefined Role	Task Group and Tasks	Workspace
Service Now Administrator		All workspaces

Table 77: Predefined Roles for Service Now Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
	<ul style="list-style-type: none"> Administration <ul style="list-style-type: none"> Service Now Devices <ul style="list-style-type: none"> Export Devices View Exposure Install Event Profile Uninstall Event Profile Delete Associate Device Groups Export Inventory Information Create On-Demand Incident Add Devices Add to Auto Submit Policy Organizations <ul style="list-style-type: none"> Modify Organization Delete Organizations Check Status View Messages Add Organization Add Member Global Settings <ul style="list-style-type: none"> SNMP Configuration Proxy Server Configuration Device Groups <ul style="list-style-type: none"> Create Device Group Modify Device Group Delete Device Groups Event Profiles <ul style="list-style-type: none"> Script Bundles <ul style="list-style-type: none"> Delete Script Bundles Set as Default Bundle Add Script Bundle View Events Show Associated Devices Add Event Profile Clone Delete Set as Default Profile Push to Devices Auto Submit Policy <ul style="list-style-type: none"> Export Incidents Report Modify Auto Submit Policy Delete Change Status Create Auto Submit Policy 	

Table 77: Predefined Roles for Service Now Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
	<ul style="list-style-type: none"> • Service Central <ul style="list-style-type: none"> • Incidents <ul style="list-style-type: none"> • Export JMB to HTML • View JMB • Export Incident Summary to Excel • View KB Article • View Case in Case Manager • View Tech Support Cases <ul style="list-style-type: none"> • View Case in Case Manager • View End Customer Cases <ul style="list-style-type: none"> • View Case in Case Manager • Update Case • Delete • Submit Case • Assign Ownership • Flag to Users • End Customer Cases • Auto Submit Policy • JMB Errors <ul style="list-style-type: none"> • Download JMB Errors • Delete • Information <ul style="list-style-type: none"> • Messages <ul style="list-style-type: none"> • Scan for Impact • Assign Ownership • Flag to Users • Delete • Assign Message to Connected Members • Device Snapshots <ul style="list-style-type: none"> • Export JMB to HTML • View JMB • Delete • Notifications <ul style="list-style-type: none"> • Create Notifications • Edit Filters and Actions • Delete • Copy • Enable/Disable 	

Table 77: Predefined Roles for Service Now Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
Service Now Unrestricted User	<ul style="list-style-type: none"> Administration <ul style="list-style-type: none"> Service Now Devices Export Devices View Exposure Service Central <ul style="list-style-type: none"> Incidents <ul style="list-style-type: none"> Export JMB to HTML View JMB Export Incident Summary to Excel View KB Article View Case in Case Manager View Tech Support Cases <ul style="list-style-type: none"> View Case in Case Manager View End Customer Cases <ul style="list-style-type: none"> View Case in Case Manager Update Case Delete Submit Case Assign Ownership Flag to Users End Customer Cases JMB Errors <ul style="list-style-type: none"> Download JMB Errors Delete Information <ul style="list-style-type: none"> Messages <ul style="list-style-type: none"> Scan for Impact Assign Ownership Flag to Users Delete Assign Messages to connected members Device Snapshots <ul style="list-style-type: none"> Export JMB to HTML View JMB Delete Notifications <ul style="list-style-type: none"> Create Notifications Edit Filters and Actions Delete Copy Enable/Disable 	Administration Service Central

Table 77: Predefined Roles for Service Now Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
Service Now Read Only User	<ul style="list-style-type: none"> Administration <ul style="list-style-type: none"> Service Now Devices Export Devices View Exposure 	Administration
	<ul style="list-style-type: none"> Service Central <ul style="list-style-type: none"> Incidents <ul style="list-style-type: none"> Export JMB to HTML View JMB Export Incident Summary to Excel View KB Article View Case in Case Manager View Tech Support Cases <ul style="list-style-type: none"> View Case in Case Manager View End Customer Cases <ul style="list-style-type: none"> View Case in Case Manager JMB Errors <ul style="list-style-type: none"> Download JMB Errors Information <ul style="list-style-type: none"> Messages <ul style="list-style-type: none"> Scan for Impact Device Snapshots <ul style="list-style-type: none"> Export JMB to HTML View JMB Notifications 	Service Central

[Table 78 on page 501](#) shows the Junos Space predefined roles for the Ethernet Design application.

Table 78: Predefined Roles for Ethernet Design Application

Predefined Role	Task Group and Tasks	Workspace
Network Engineer	<ul style="list-style-type: none"> Port Profiles <ul style="list-style-type: none"> Create Port Profile Provision Port Profile Manage VLANs <ul style="list-style-type: none"> Create VLAN Manage QFabric Node Groups <ul style="list-style-type: none"> Create a Node Group Manage QFabric Port Groups <ul style="list-style-type: none"> Create a Port Group 	EZ Design

Related Documentation • [Role-Based Access Control Overview on page 479](#)

- [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)
- [Managing Roles on page 503](#)
- [Creating a User-Defined Role on page 505](#)
- [Modifying User-Defined Roles on page 506](#)
- [Deleting User-Defined Roles on page 507](#)
- [Creating User Accounts on page 509](#)
- [Viewing Users on page 516](#)
- [Viewing User Statistics on page 524](#)

Managing Roles Overview

Roles define the application workspace tasks a user is assigned by the Super Administrator and User Administrator to perform in Junos Space Network Management Platform. Users represent an individual in a security domain who is authorized to log into Junos Space Network Management Platform and perform application workspace tasks according to predefined and user-defined roles.

The administrator can create a user account and assign tasks based on read-only predefined roles and read-write user-defined task roles. See [“Creating User Accounts” on page 509](#) and [“Predefined Roles Overview” on page 481](#). You can create user-defined tasks first, then create a user account, or create a user account, then modify the account afterward. You can also use an existing user account as a template to assign roles to users with similar job types.

The **Users > User Accounts** task allows the Super Administrator or User Administrator to manage all roles by performing the following user role tasks:

- View all predefined and user-defined roles on the **Users > Roles** inventory page. See [“Managing Roles” on page 503](#).
- Create user-defined roles from the **Users > Roles > Create Role** task. See [“Creating a User-Defined Role” on page 505](#).
- Modify user-defined roles using **Modify Role** in the **Users > Roles** inventory page. See [“Modifying User-Defined Roles” on page 506](#).
- Delete user-defined roles using **Delete Roles** in the **Users > Roles** inventory page. See [“Deleting User-Defined Roles” on page 507](#).
- Tag predefined and user-defined roles to group them for performing actions all at once. Use **Tag It** in the **Users > Roles** inventory page Actions menu. See [“Tagging an Object” on page 695](#).
- View all tags that exist on roles using **View Tags** in the **Users > Roles** inventory page Actions menu. See [“Viewing Tags for a Managed Object” on page 696](#)

Related Documentation

- [Role-Based Access Control Overview on page 479](#)

- [Predefined Roles Overview on page 481](#)
- [Creating User Accounts on page 509](#)
- [Managing Roles on page 503](#)
- [Creating a User-Defined Role on page 505](#)
- [Modifying User-Defined Roles on page 506](#)
- [Deleting User-Defined Roles on page 507](#)

Managing Roles

A role is a description of tasks a user can perform in Junos Space Network Management Platform to allow access to application workspaces. The **Users > Roles** inventory page allows the Super Administrator or the User Administrator to view all predefined and user-defined roles that exist for Junos Space applications. The administrator should understand all predefined roles and create any user-defined roles before creating users.

Viewing User Role Details

The **Roles** inventory page displays all predefined and user-defined roles in a tabular view.

Each role is represented by a row in the table. Roles are listed in the table in ascending alphabetical order by role title, description, and tasks assigned. You can show or hide table columns and sort records in ascending or descending order.

You can search for roles by typing the first letters of the role title in the search box. Role title starting with the first letters you type are listed.

To view a user role detail summary:

1. Double-click a role.

The Role Details Summary page appears.

The page displays the workspace, and workspace tasks.

2. Click the expander button **[+]** to view subtasks.
3. Click **OK**.

Performing Manage Roles Commands

The commands you can perform on predefined and user-defined roles are located in the Actions menu or by right-clicking that role. You can only perform the **Modify Role** and **Delete Roles** commands on read-writeable user-defined roles. You cannot manipulate read-only predefined roles. To perform a command, you must first select the role.

The following commands are included in the **Modify Role** Actions menu:

- **Modify Role**—Modify the selected user-defined role title, description, and application workspace task. You cannot modify predefined roles. For more information, see [“Modifying User-Defined Roles” on page 506](#).
- **Delete Roles**—Delete the selected user-defined role. You cannot delete predefined roles. For more information, see [“Creating a User-Defined Role” on page 505](#).
- **Tag It**—Tag one or more selected inventory objects, see [“Tagging an Object” on page 695](#).
- **View Tags**—View a list of tags that exist on a selected inventory object. For more information, see [“Viewing Tags for a Managed Object” on page 696](#).
- **Untag It**—Untag a tag that has been applied to an inventory object, see [“Untagging Objects” on page 697](#).
- **Clear All Selections**—Clear any user role selections you made on the Manage Roles inventory page. Use the Select: Page in the Manage Roles page title bar to select all roles at once.

**Related
Documentation**

- [Role-Based Access Control Overview on page 479](#)
- [Predefined Roles Overview on page 481](#)
- [Creating User Accounts on page 509](#)
- [Creating a User-Defined Role on page 505](#)
- [Modifying User-Defined Roles on page 506](#)
- [Deleting User-Defined Roles on page 507](#)

Manage User-Defined Roles

- [Creating a User-Defined Role on page 505](#)
- [Modifying User-Defined Roles on page 506](#)
- [Deleting User-Defined Roles on page 507](#)

Creating a User-Defined Role

Junos Space Network Management Platform provides a number of read-only predefined roles you, the Super Administrator, System Administrator, or User Administrator can use to create user log in, access, and perform tasks in application workspaces. You can also create read-write user-defined roles that conform to user responsibilities and access privileges required on your network. You can modify and delete only user-defined roles that you create. You cannot modify or delete predefined roles.

To create a user-defined role:

1. Select **Users > Roles** and click the Create Role icon on the menu bar.

The Create Role page appears, allowing you to select workspaces and associated tasks from all deployed applications.

2. In the **Title** text box, type a user-defined role name.

The role title cannot exceed 32 characters. The title can only contain letters, numbers, and can include a hyphen (-), underscore (_), or period (.).

3. In the **Description** box, type a user-defined role description.

The role description cannot exceed 256 characters

4. Select an application workspace from the application selection ribbon.

Mouse over an application workspace icon to view the application and workspace name. You can select one or more workspaces per user-defined role. An expandable/collapsible tree of associated tasks appear below the selection ribbon for you to modify specific tasks you want included in the Task Summary pane.

5. Select the specific task(s) you want for the user-defined role. All application workspace tasks are by default deselected in the task tree.

Only the currently edited application workspace node is expanded in the Task Summary pane; previously selected workspace nodes are collapsed. You can expand other workspace nodes manually.

Selecting the top node or workspace selects or deselects the whole task tree. Selecting any task node automatically selects its decedents. Selecting any task node automatically selects its parent and grandparent.

Only the currently active task tree appears in the Task Summary pane.

In the Task Summary pane, the top level application node in the tree is bold-italic; the second level workspace tree node is bold.

6. Click **Create**.

The user-defined role is created, saved, and appears in the Roles inventory page.

Scroll down or search to view it.

You cannot create or save a user-defined role when the workspace tasks are not selected.

**Related
Documentation**

- [Predefined Roles Overview on page 481](#)
- [Managing Roles on page 503](#)
- [Modifying User-Defined Roles on page 506](#)
- [Deleting User-Defined Roles on page 507](#)
- [Creating User Accounts on page 509](#)

Modifying User-Defined Roles

The Super Administrator and the User Administrator can modify user-defined roles that have been created. You can modify the role description, application workspace, and the selected tasks. You cannot modify the role title or predefined roles.

To modify a user-defined role:

1. Select **Users > Roles**.

The Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined role you want to modify.

3. Select **Modify Role** from the Actions menu.

4. Modify the part of the user-defined role that you want: description, application workspace, or tasks.

The role title cannot exceed 32 characters. The title can only contain letters, numbers, and can include a hyphen (-), underscore (_), or period (.).

The role description cannot exceed 256 characters

5. Click **Modify**.

The modified user-defined role is updated in the Manage Roles inventory page.

- Related Documentation**
- [Predefined Roles Overview on page 481](#)
 - [Creating User Accounts on page 509](#)
 - [Managing Roles on page 503](#)
 - [Managing Roles Overview on page 502](#)
 - [Creating a User-Defined Role on page 505](#)
 - [Deleting User-Defined Roles on page 507](#)

Deleting User-Defined Roles

The Super Administrator and the User Administrator can delete user-defined roles from the **Roles** inventory page only if they are not being used by other users. You cannot delete pre-defined roles.

To delete a user-defined role:

1. Select **Users > Roles**.

The Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined role(s) you want to delete.
3. Select **Delete Roles** from the Actions menu.

The Delete Roles dialog box appears.

4. Click **Delete**.

The role is deleted from the Roles inventory page. If the role is used by other Junos Space Network Management Platform users, you cannot delete the role. A warning message appears.

- Related Documentation**
- [Predefined Roles Overview on page 481](#)
 - [Managing Roles on page 503](#)
 - [Creating a User-Defined Role on page 505](#)
 - [Managing Roles Overview on page 502](#)
 - [Modifying User-Defined Roles on page 506](#)
 - [Creating User Accounts on page 509](#)

CHAPTER 54

Manage Users

- [Creating User Accounts on page 509](#)
- [Disabling and Enabling Users on page 515](#)
- [Viewing Users on page 516](#)
- [Modifying a User on page 520](#)
- [Deleting Users on page 522](#)
- [Changing User Passwords on page 522](#)
- [Clearing User Local Passwords on page 523](#)
- [Viewing User Statistics on page 524](#)

Creating User Accounts

The Super Administrator and the User Administrator can create Junos Space Network Management Platform user accounts that specify the credentials and predefined roles allowing users to log in and use Junos Space applications, workspaces, and tasks. Each user account must include:

- Login ID
- Password
- First name
- Last name

For each user, you can assign roles that define the tasks and objects (devices, users, services, and so forth) that the user can access and manage. You can assign multiple roles to a single user and assign the same role to multiple users.

You can also assign permissions to users to limit their access to only specified objects within the workspace that the assigned role controls (see [“Managing Permission Labels Overview” on page 701](#)).

The **Use Same Roles Assigned To** option allows you to quickly create multiple user accounts without having to reselect the same predefined roles. The predefined user roles that are available are displayed on the Create User pages. You can also distinguish whether a user has access to GUI, API, or both.

User accounts are subdivided into three areas—General, Role Assignment, and Permission Assignment. There are links to these areas in the upper right corner of the Create User page. You might need to scroll horizontally in order to see the links.



NOTE: If you do not use Permission Labels, a user can access all the objects that the assigned role controls within the workspace.

Creating a New User Account

To create a new user account:

1. Select **Network Management Platform > Users > User Accounts**.

The Users > User Accounts page appears.

2. Click the Create User icon [+] in the upper menu bar to display the Create User page.

The Create User page appears, displaying the fields for the General area.

3. In the Login ID box, enter a login ID for the new Junos Space user account.

This can be an e-mail address. If it is, it is not mandatory that the login ID match the e-mail address entered in the Email field. The login ID cannot exceed 128 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers, as well as the @ and the period (.). You cannot have two users with the same login ID.



NOTE: Junos Space Network Management Platform does not permit you to create the user, admin. It throws the following error message:
Username admin is reserved in Space. Please do not create user with username, admin.

4. Display the rules for password creation by mousing over the information icon (small blue [i]) next to the Password field. For information on configuring the password rules, see [“Configuring Password Settings for Junos Space Network Management Platform” on page 628](#).

Type and confirm the local password.



NOTE: All passwords in Junos Space Network Management Platform are case-sensitive.

5. In the First Name box, enter the user's first name.

The name cannot exceed 32 characters.

6. In the Last Name box, enter the user's last name.

The name cannot exceed 32 characters.

7. (Optional) In the Email box, enter the user's e-mail address.

This need not be the same as the login ID, if the login ID was an e-mail address.

8. (Optional) Clear the Use global settings check box to configure the maximum number of concurrent UI sessions that should be allowed for this user.

By default, this check box is selected, which means that the global concurrent UI sessions limit applies to this user. This limit is displayed in the Maximum concurrent UI sessions text box. For more information about how to configure this limit globally, see [“Limiting User Sessions” on page 513](#).

9. (Optional) In the Maximum concurrent UI sessions text box, enter the maximum number of concurrent UI sessions that should be allowed for this user. By default, the value of this field is set to the global concurrent UI sessions limit. For more information about how to configure this limit globally, see [“Limiting User Sessions” on page 513](#).

Typically, this text box is unavailable (that is, when the Use global settings check box remains selected). To make any configuration changes, clear the Use global settings check box first.

You can enter a value from 0 through 999. Entering 0 (zero) means that there is no restriction to the number of concurrent UI sessions allowed per user. However, the system performance maybe degraded if you allow unlimited sessions.

10. (Optional) In the Image File box, upload the user’s photo ID:

- a. Use the Browse button to locate the user’s photo ID file.

You can upload image file formats with the following extensions: .bmp, .gif, .jpg, and .png.

- b. Click **Upload**.

Junos Space Network Management Platform uploads and saves the photo ID file for the user account.

If you do not want to assign the user roles or the permissions at this point, you can click **Finish** to create the user account without assigning any roles. . If you want to assign user roles now, proceed to the next step by clicking **Next**.

11. (Optional) In the X509 Cert File, upload the user’s X.509 certificate file.

- a. Use the Browse button to locate the user’s X.509 certificate file on your local system.

You can upload certificate file formats with the following extensions: .der, .cer, and .crt.

- b. Click **Upload**.

Junos Space Network Management Platform uploads and saves the certificate file for the user account.

12. To assign roles to the new user, click **Role Assignment** on the upper right, and do one of the following:

- Select the **Use Same Roles Assigned to** check box and select the name of an existing user whose roles you want to assign to the new user.



TIP: Enter one or more characters of the username in the Use Same Roles Assigned to search box to find the user and select the username. The assigned roles appear in the Selected roles list. You can modify the new user's role assignments by adding or removing roles from the Selected Roles column.

or

- Use the double list box to select predefined roles for the user. Select one or more roles from the Available list box. Selected roles appear in the Selected list box. Use the right arrow to move the selected roles to the Selected list box. Use the left arrow to move roles from the Selected list box back to the Available list box. You can also double-click a role to select or remove it. You see the details of selected roles appear in the right pane of the page.

You can also create user-defined roles for users. For more information, see [“Creating a User-Defined Role” on page 505](#).



NOTE: The minimum role required for configuring a user for IBM Systems Director and Junos Space Launch in Context (LIC) is Device Manager.

- Select the **GUI Access** and **API Access** check-boxes depending on the type of access you want to allow for the user.

By default, the user gets access to both GUI and API. You should select at least one access type to successfully create a user account.

If you do not want to assign the user permissions at this point, you can click **Finish** to create the user account without assigning any permissions. If you want to assign user permissions now, proceed to the next step by clicking **Next**.

13. To assign permission labels to the new user, click **Permission Assignment** on the upper right, and do one of the following:

- Select the **Use Same Permission Labels Assigned to** check box and select the name of an existing user whose permission labels you want to assign to the new user.



TIP: Enter one or more characters of the username in the Use Same Permission Labels Assigned to search box find the user and select the username. The assigned permission labels appear in the Selected list box. You can modify the new user's permission label assignments by adding or removing permission labels from the Selected column.

or

- Use the double list box to select permission labels for the user. Select one or more permission labels from the Available list box. Selected permission labels appear in the Selected list box. Use the right arrow to move the selected labels to the Selected list box. Use the left arrow to remove labels from the Selected list box back to the Available list box. You can also double-click a label to select or remove it. You see the details of selected labels appear in the right pane of the page.



TIP: You can also create permission labels for users. Do not forget to attach a newly created permission label to an object as well as assigning it to a user. For more information, see [“Assigning Permission Labels” on page 705](#).

14. Click **Finish** to create the user account with the assigned roles and permissions, if applicable.

The new user account is created in the Junos Space Network Management Platform database. You see the new user account on the Manage Users inventory page.

Limiting User Sessions

You can configure the maximum number of concurrent UI sessions that should be allowed for a user, both globally and at the user-level, which can help you improve the system performance.

When this limit is configured, any login attempt from GUI is validated against this limit and the user is prevented from logging in if the concurrent user session limit is reached for that user. The user is notified with the following message: “You are not allowed to login since your sessions exceed the configured limit.”



NOTE: If you are a **super** user, this concurrent user session limit does not apply and you are allowed to log in even when you have exceeded this limit.

The global configuration limit is applicable to all the users. However, if you have a user level configuration, then this configuration takes precedence over the global configuration for that specific user. For example, if you set the global limit to 5 and at the user-level to 10 for user A, then user A is prevented from logging in at the 11th attempt. However, if the global limit is set to 10 and the user limit is set to 5, then the user is rejected at the 6th login attempt.

In instances where you have the same user configured locally as well as remotely (that is, in TACACS or RADIUS server), the concurrent UI sessions limit that is most restrictive takes effect. For example, if you have set the sessions limit to 1 in the TACACS server and to 2 in Junos Space Network Management Platform for user B, then user B is prevented from logging in at the second attempt. When the session limit is set to 2 in the TACACS server and to 1 in Junos Space Network Management Platform, you can see the same results of user being rejected at the second attempt.



NOTE: What constitutes a browser session?

- Accessing the Junos Space GUI from two tabs of the same browser is considered as a single session
 - An incognito tab is considered as another session
 - Accessing the GUI from another browser's tabs is considered as another session
 - Configuring any Junos Space parameters using APIs is not considered as a session
-

To set the concurrent UI sessions limit, globally (that is, for all the users):

1. Select **Network Management Platform > Applications**.

The Administration > Applications page appears.

2. Select **Network Management Platform**.

3. Select **Modify Application Settings** from the **Actions** menu.

The Modify Network Management Platform Settings page appears.

4. Click **User**.

5. In the **Maximum concurrent UI sessions per user** text box, enter the maximum number of concurrent UI sessions that should be allowed per user.

By default, a user is allowed up to 5 concurrent UI sessions. You can enter a value from 0 through 999. Entering 0 (zero) means that there is no restriction to the number of concurrent UI sessions allowed per user. However, the system performance may be degraded if you allow unlimited sessions.

To set the concurrent session limit at the user level:

1. Select **Network Management Platform > Users > User Accounts**.

The Users > User Accounts page appears.

2. Click the Create User icon [+] in the upper menu bar to display the Create User page.

The Create user page appears.

3. (Optional) Clear the Use global settings check box to configure the maximum number of concurrent UI sessions that should be allowed for this user.

By default, this check box is selected, which means that the global concurrent UI sessions limit applies to this user. This limit is displayed in the Maximum concurrent UI sessions text box.

4. (Optional) In the Maximum concurrent UI sessions text box, enter the maximum number of concurrent UI sessions that should be allowed for this user. By default, the value of this field is set to the global concurrent UI sessions limit. You can enter a value from 0 through 999. Entering 0 (zero) means that there is no restriction to the number

of concurrent UI sessions allowed per user. However, the system performance may be degraded if you allow unlimited sessions.

Typically, this text box is unavailable (that is, when the Use global settings check box remains selected). To make any configuration changes, clear the Use global settings check box first.

5. Click **Finish**.

For existing Space users, from the User Accounts page, select the user and click **Modify User** to make any changes to the concurrent UI sessions limit for that user.



NOTE: The changes that you do to the concurrent UI sessions limit (either at the global-level or at the user-level) do not impact the existing sessions. That is, this limit is validated against the next user log in only.

For troubleshooting, see the `/var/log/jboss/server.log` file, which captures any internal errors. Also, see the audit logs, which captures the following actions by Administrator:

- Configuration changes to the global concurrent UI sessions limit
- When the global configuration is overridden at the user-level
- When the concurrent UI sessions limit is reached for a user

Disabling and Enabling Users

Disable a user to prevent the user from logging in to the system.

By default, all users are enabled.

Super-users cannot be disabled.

The action of enabling or disabling a user generates an audit log entry.

On the User Accounts inventory landing page, user status appears in the Status column, which shows icons for enabled or disabled status. The User Detail Summary page also indicates a user's status.

When a user is disabled, the user sees the message “This account is disabled” when the user tries to log in to the system. If the user is active at the time the user is disabled, the system logs the user off and displays to the user a message saying that the user account is disabled. In both cases, a disabled user's attempt to log in generates an audit log entry.

You cannot disable your own user account.

To disable or enable one or more users:

1. Select **Users > User Accounts**.

The User Accounts page appears.

2. Select one or more users to disable or enable.



NOTE: If both the Enable and the Disable actions are unavailable, you have selected a super-user.

3. Select **Disable Users** or **Enable Users** from the Actions menu.

The Disable or Enable Users confirmation dialog box appears, displaying the list of users to whom the selected action will be applied. Users you selected, but who do not appear in the list, will not have the action applied to them. Only those users who are not already in the state to which you want to convert them can be enabled or disabled. If you selected disabled users to disable again, a message appears, telling you how many users' status will not change.

4. Verify the list of users that you want to disable or enable, and click **Disable / Enable**, respectively.

All selected user accounts are disabled or enabled.

Related Documentation

- [Creating User Accounts on page 509](#)
- [Modifying a User on page 520](#)
- [Viewing Users on page 516](#)
- [Junos Space Audit Logs Overview on page 531](#)

Viewing Users

The User Accounts inventory page displays all of the Junos Space Network Management Platform users who have accounts. To add new users, you must have administrator privileges. To add a new user, see [“Creating User Accounts” on page 509](#). Users have Junos Space access based on predefined user roles (see [“Predefined Roles Overview” on page 481](#)). For more information about how to manipulate inventory page data, see [“Junos Space User Interface Overview” on page 9](#).

This topic describes how to view the inventory of users and their details. To do this, select **Users > User Accounts**.

The User Accounts page appears.

Users are displayed in a table sorted by default by user name. Each user occupies a row in the User Accounts table. The table's column headings are User Name, First Name, Last Name, Email, User Type, GUI/API Access, and Status.

The status bar at the bottom of the page shows the range of objects being displayed, for example, you might see *Displaying 1-30 of 113*. In addition, the Show Items drop-down list enables you to select the number of items to display per page: 10, 20, 40, 60, 80, 100.

The filter function, described here, enables you to get around the difficulty of not being able to view all users on a single page.

- [Sorting Columns on page 517](#)
- [Displaying or Hiding Columns on page 517](#)
- [Filtering on Columns on page 518](#)
- [Viewing User Details on page 518](#)
- [Performing Manage User Commands on page 519](#)

Sorting Columns

The columns in the Manage Users table, that is, the Manage Users inventory landing page, can be sorted to display ascending or descending order.

To sort the contents of a column,

1. Click the arrow to the right of any column heading.

A list with the following menu options appears:

- Sort Ascending
- Sort Descending
- Columns
- Filters

2. Select Sort Ascending or Sort Descending.

The sequence of objects in the column changes to reflect your choices.

Displaying or Hiding Columns

The columns in the Manage Users table, that is, the Manage Users inventory landing page, can be displayed or hidden as required.

To display or hide a column,

1. Click the arrow to the right of any column heading.

A list with the following menu options appears:

- Sort Ascending
- Sort Descending
- Columns
- Filters

2. Select Columns.

A list with menu options corresponding to all the available column headings appears, a check box next to each heading. The check boxes for the headings that are displayed are checked, those that are hidden are not checked.

3. Select or deselect the headings as desired.

The table view changes to reflect your choices.

Filtering on Columns

The contents of the columns in the Manage Users table, that is, the Manage Users inventory landing page, can be filtered as required. For very comprehensive descriptions, see [“Filtering Inventory Pages” on page 27](#); here are more basic instructions:

To filter on one or more columns, for each:

1. Click the arrow to the right of any column heading.

A list with the following menu options appears:

- Sort Ascending
- Sort Descending
- Columns
- Filters

2. Select Filters.

The filter field appears, with a Go button to the right of it.

3. Enter the filter criteria and click **Go**.

On applying the filter(s), the table contents shrink to display the values that match the filter applied. The criteria by which the display is filtered and the column heading appear just above the table.



NOTE: Filters applied across multiple columns have an additive effect; that is, each succeeding filter further restricts the display.

4. To remove a filter, click the [x] to the right of the filter criteria shown just above the table.

Viewing User Details

To view more detailed user information:

- Select a user and click the Quick View icon in the menu bar.

To the right of the table appear the selected user's:

- Login ID
 - First Name
 - Last Name
 - Email
- Double-click a user row in the table.

The User Detail Summary page appears, showing the information described in [Table 79 on page 519](#).

Table 79: User Detail Summary Page

Data	Description
Login ID	The login username. This could be an email address, but it does not need to match the email address that might be provided in the field of that name.
First Name	The first name of the user.
Last Name	The last name of the user.
Email	(Optional) The user's email account. The email address provided here need not match the login ID, if that is also an email address.
User Type	Type of the user. Local users are shown as Local and remote users are shown as ReadOnly.
Status	Enabled or disabled. Users are enabled by default. Disabling a user is not the same as deleting a user.
GUI Access	Whether the user has GUI access.
API Access	Whether the user has API access.
Use Global Settings	Whether the global settings must be used.
Maximum concurrent UI sessions	Maximum number of concurrent UI sessions.
Assigned Roles	The predefined user roles assigned to user.
Assigned Permission Labels	The work spaces a user can use and tasks a user can perform based on the permission labels assigned to the user and to the objects..
Role Summary	Name of the application(s) to which the role(s) belong(s), and list of permissions attached to the role(s).

To close the User Detail Summary, click **OK** or the [x] in the upper right corner of the page.

Performing Manage User Commands

You can perform the following actions from the Manage Users page:

- Modify User—See [“Modifying a User” on page 520](#)
- Delete User—See [“Deleting Users” on page 522](#)
- Tag It—[“Tagging an Object” on page 695](#)
- View Tags—[“Viewing Tags for a Managed Object” on page 696](#)

Related Documentation

- [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)
- [Creating User Accounts on page 509](#)
- [Deleting Users on page 522](#)
- [Modifying a User on page 520](#)
- [Viewing User Statistics on page 524](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)
- [Filtering Inventory Pages on page 27](#)

Modifying a User

A Super Administrator or User Administrator can modify any user account in Junos Space Network Management Platform. The only attribute that cannot be modified is the login ID.

The Modify User pages have three areas, General, Role Assignment and Permission Assignment, in which user information is grouped accordingly. Each user account can have multiple roles and a role can be associated with multiple users. .

To modify an existing user account:

1. Select **Users > User Accounts**.

The **User Accounts** inventory page appears.

2. From the inventory page, select the user account that you want to modify. For instructions on filtering and sorting, see [“Viewing Users” on page 516](#).

You can modify only one user account at a time.

3. From the menu bar above the table, select the Modify icon, the pencil.

The **Modify User** page appears, displaying the General area by default, with the existing account information for that user.

4. You can change any of the information in the General area except the login ID.
 - To view the rules governing password creation, mouse over the information icon, the small blue [i] to the right of the Password field. To configure the password rules, see [“Configuring Password Settings for Junos Space Network Management Platform” on page 628](#).
 - To change the user name, enter a new name in the First Name and Last Name boxes.
 - To change the email account, enter a new email address in the Email field.

To upload an image file:

- a. Use the **Browse** button to locate the new user photo ID file.

You can upload BMP, GIF, JPG, and PNG image file formats.

- b. Click **Upload**.

Junos Space Network Management Platform updates the photo ID file for the user account.

To add or remove role assignments:

- a. Click **Role Assignment** on the upper right of the page, or click **Next** on the bottom right of the page.
- b. To add role assignments, select one or more roles from the Available Roles column and click the right arrow to move the roles to the Selected Roles column.
- c. To remove role assignments, select one or more roles from the Selected Roles column and click the left arrow to move the roles to the Available Roles column.
- d. Click **Next** at the bottom of the page or **Permission Assignment** at the top of the page to modify the selected user's permission assignments, or click **Finish** at the bottom of the page to complete the modification.

To add, remove, or change permission assignments:

- a. Click **Permission Assignment** on the upper right of the page, or click **Next** on the bottom right of the page.
- b. The easiest way to change permission assignments is to select the **Use Same Permission Label Assigned to** check box.

The **Use Same Permission Label Assigned to** dropdown list is activated. Select the user on which the current user is to be modeled from the drop-down list.

- c. To add permission assignments, select one or more assignments from the Available column and click the right arrow to move the roles to the Selected column.
- d. To remove role assignments, select one or more roles from the Selected Roles column and click the left arrow to move the roles to the Available Roles column.
- e. Click **Finish** at the bottom of the page to complete the modification.

Junos Space Network Management Platform updates the user account with the changes you specified.

**Related
Documentation**

- [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)
- [Creating User Accounts on page 509](#)
- [Deleting Users on page 522](#)
- [Viewing Users on page 516](#)
- [Assigning Permission Labels on page 705](#)

Deleting Users

When a Junos Space Network Management Platform user leaves your organization or no longer needs access to the system, the administrator should delete the existing user account.

To delete one or more users:

1. Select **Users > User Accounts**.

The User Accounts inventory page appears, displaying all user accounts.

2. Select one or more users to delete.
3. From the menu bar above the table, select the **Delete Users** icon.

The Delete Users confirmation dialog box appears.

4. Verify the list of users that you want to delete and click **Delete**.

All selected user accounts are removed from the Junos Space Network Management Platform database and the User Accounts inventory page.

- Related Documentation**
- [Creating User Accounts on page 509](#)
 - [Modifying a User on page 520](#)
 - [Viewing Users on page 516](#)

Changing User Passwords

Users who are logged in to Junos Space Network Management Platform can change their account passwords by using the User Preferences icon on the Junos Space application banner. No particular Junos Space role is required for users to change their passwords.

Beginning with Junos Space Network Management Platform Release 12.1, Junos Space has implemented a default standard for passwords that is compliant with industry standards for security.



NOTE: Upgrading to Junos Space Platform 12.1 or later causes the default standard to take effect immediately. All local users will get password expiration messages the first time they log in after the update.



NOTE: If you do not have a local password set, you will not be able to set or change it.



NOTE: Using User Preferences to change your password only works for local passwords. The change does not affect any passwords that an administrator might have configured for you on a remote authentication server.

To change your user password:

1. Click the User Preferences icon on the upper right, in the Junos Space application banner.

The User Preferences – Change Password dialog box appears.

2. Type your old password.
3. Display the rules for password creation by mousing over the information icon (small blue [i]) next to the password field.

Type your new password.

4. Retype your password to confirm it.
5. Click **OK**.

You are logged out of the system. You have to log in again using your new password. Other sessions for the same user are unaffected until the next login.

**Related
Documentation**

- [Creating User Accounts on page 509](#)
- [Logging In to Junos Space on page 3](#)
- [Configuring Password Settings for Junos Space Network Management Platform on page 628](#)

Clearing User Local Passwords

The Clear Local Passwords command lets you remove the local password you assign to users with remote or remote-local authentication. This setting allows an emergency password (authentication server down) if in Remote mode, or allows the user to be handled locally (remote authentication fails) if in Remote-Local mode.

To remove one or more user local passwords, you must have User Administration privileges.

To remove a user local password:

1. Select **Users > User Accounts**.

The User Accounts inventory page appears.

2. Select one or more users for which you want to remove a local password.
3. Select **Clear Local Passwords** from the Actions menu.

The **Delete Users** dialog box appears.

4. Click **Clear Passwords**.

- Related Documentation**
- [Viewing Users on page 516](#)
 - [Creating User Accounts on page 509](#)
 - [Modifying a User on page 520](#)
 - [Creating a Remote Authentication Server on page 670](#)

Viewing User Statistics

You can view the percentage and the number of Junos Space Network Management Platform users that have been assigned to a role.

- [Viewing the Number of Users Assigned by Role on page 524](#)

Viewing the Number of Users Assigned by Role

To view the percentage of total users that have been assigned to a predefined role:

1. Select **Users**.

The Users inventory page appears.

Junos Space Network Management Platform displays a bar chart showing users by assigned role.

The bar chart displays the number of users assigned to each role that has one or more assigned users.

2. To view the number of users assigned to a specific role, mouse over the role in the chart.
3. To display an inventory page of users assigned to a specific role, click on the segment of the chart that represents the role.

- Related Documentation**
- [Role-Based Access Control Overview on page 479](#)
 - [Viewing Users on page 516](#)
 - [Creating User Accounts on page 509](#)
 - [Deleting Users on page 522](#)

Manage Remote Profiles

- [Creating a Remote Profile on page 525](#)

Creating a Remote Profile

To create a remote profile:

1. Select **Users > Remote Profiles**.
The Remote Profiles page is displayed.
2. Select the **Create Remote Profile** icon on the menu bar.
The Create Remote Profile page is displayed.
3. In the Name field, enter a name for the remote profile.
Ensure that you enter the name without spaces or special characters.
4. In the Description field, enter a description for the remote profile.
5. Select the **GUI Access** and **API Access** check-boxes depending on the type of access you want to allow for the remote profile.

By default, the remote profile gets access to both GUI and API. You should select at least one access type to successfully create a remote profile.
6. Use the double list box to select predefined roles for the remote profile. Select one or more roles from the Available list box. Selected roles appear in the Selected list box. Use the right arrow to move the selected roles to the Selected list box. Use the left arrow to move roles from the Selected list box back to the Available list box. You can also double-click a role to select or remove it. You see the details of selected roles appear in the right pane of the page.
7. Click **Create**.

Remote profiles can be modified, deleted, and tagged.



NOTE: A user will not be allowed to log in if the remote profile specified in the remote server does not exist in the local database. A message "No roles assigned for this user" is displayed on the login screen. This information is logged as an audit log.

**Related
Documentation**

- [Predefined Roles Overview on page 481](#)
- [Managing Roles on page 503](#)
- [Modifying User-Defined Roles on page 506](#)
- [Deleting User-Defined Roles on page 507](#)
- [Creating User Accounts on page 509](#)

User Sessions

- [Terminating User Sessions on page 527](#)

Terminating User Sessions

As a Junos Space User administrator, you can view and terminate user sessions before starting a maintenance cycle to minimize the risk of system inconsistency. You can view the list of users who are logged in along with details of IP address of the client from which they are logged in and the duration of their sessions. You can select one or more users to terminate their sessions.

When you trigger a session termination, the users whose sessions you have chosen for termination will be notified. The notification includes the date and time when the sessions will be terminated. As a user whose session will be terminated, you will be automatically logged out and redirected to login page at the scheduled date and time.

To terminate user sessions:



NOTE: You will not be able terminate sessions of a user with a username *super*.

When you delete or disable a user in Junos Space Network Management Platform, the user's sessions will terminate automatically. If a user closes the session before the scheduled time for terminating the session and logs back in, the new session is not considered for session termination.

1. Select **Users > User Sessions**.

The User Sessions page appears. This page displays the user name, IP address, session start time, and the session duration of the sessions that are currently logged in.

2. Select one or more users whose sessions you want to terminate.
3. Select **Terminate User Session** from the Actions menu.

The Terminate User Session window is displayed. This window displays the user sessions that you have selected to terminate and the IP address from which the users are logged in currently.

4. Select the **Schedule at a later time** check-box to terminate the user sessions at a future point in time.
5. Select the appropriate date and time for terminating sessions from the date and time menus, respectively.
6. Click **OK**.

A job is created to terminate the sessions selected for session termination. When the job is scheduled, the users whose sessions you have selected for terminating will receive a pop-up message displaying the date and time you have specified for terminating their sessions.

**Related
Documentation**

- [Creating User Accounts on page 509](#)
- [Predefined Roles Overview on page 481](#)

PART 11

Audit Logs

- [View on page 531](#)
- [Archive / Purge on page 539](#)
- [Export on page 543](#)

CHAPTER 57

View

- [Junos Space Audit Logs Overview on page 531](#)
- [Viewing Audit Logs on page 532](#)
- [Viewing Audit Log Statistics on page 534](#)
- [Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel on page 536](#)

Junos Space Audit Logs Overview

Audit logs provide a record of Junos Space Network Management Platform login history and user-initiated tasks that are performed from the user interface. From the Audit Logs workspace, you can monitor user login/logout activity over time, track device management tasks, view services that were provisioned on devices, and so forth. Junos Space Network Management Platform audit logging does not record non-user initiated activities, such as device driven activities, and is not designed for debugging purposes. User-initiated changes made from the Junos Space CLI are logged but are not recorded in audit logs.

Administrators can sort and filter on audit logs to determine which users performed what actions on what objects at what time. For example, an Audit Log administrator can use audit log filtering to track the user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, or monitor user login/logout activity over time.

To use the audit log service to monitor user requests and track changes initiated by users, you must have the Audit Log Administrator role (see [“Managing Roles Overview” on page 502](#)).



NOTE: Audit Logging is not currently supported for Ethernet Design. However, from version 12.1 onward, audit logging is supported for Service Now.

Over time, the Audit Log administrator will archive a large volume of Junos Space Network Management Platform log entries. Such log entries might or might not be reviewed, but they must be retained for a period of time. The Archive Purge feature helps you manage your Junos Space Network Management Platform log volume, allowing you to archive log files and then purge those log files from the Junos Space Network Management Platform database. For each Archive Purge operation, the archived log files are saved in

a single file, in CSV format. The audit logs can be saved to a local server (the server that functions as the active node in the Junos Space Network Management Platform fabric) or a remote network host or media. When you archive data to a local server, the archived log files are saved to the default directory `/var/lib/mysql/archive`.

The Audit Logs Export feature enables you to download audit logs in CSV format so that you can view the audit logs in a separate application or save them on another machine for further use, without purging them from the system.

**Related
Documentation**

- [Archiving and Purging Audit Logs on page 539](#)
- [Viewing Audit Logs on page 532](#)
- [Exporting Audit Logs on page 543](#)

Viewing Audit Logs

Audit logs are generated for login activity and tasks that are initiated from the Junos Space Network Management Platform and Network Activate, as well as Service Now. The View Audit Logs page displays all tasks.

To view audit logs, you must have Audit Log Administrator privileges.



NOTE: Audit Logging is not currently supported by the Ethernet Design application.

You view audit logs in Junos Space Network Management Platform only in tabular view. For more information about how to manipulate inventory page data, see [“Junos Space User Interface Overview” on page 9](#).

Viewing Audit Log Details

The Audit Log Details dialog box displays information about the task that was logged, including information about the objects affected by the task.

To view detailed audit log information:

- If an audit log entry does not include a job ID, double-click a table row for the audit log entry. The Audit Log Details dialog box displays information about the task that was logged, including information about the objects affected by the task. Click **OK** to close the Audit Log Detail dialog box.
- If an audit log entry includes a Job ID, click the Job ID link in the audit log row. The Job Manager Inventory page displays information about the job. If this job is recurring, then it will display information about all recurrences of this job. Click **Return to Audit Logs** to close the Job Manager inventory page and return to the audit logs table.

The fields displayed in the Audit Logs table are described in [Table 80 on page 533](#).

Table 80: Detailed Audit Logs Information and View Audit Log Table Columns

Field	Description
User Name	The login ID of the user that initiated the task.
User IP	The IP address of the client computer from which the user initiated the task.
Application	The application from which the user initiated the task.
Workspace	The workspace from which the user initiated the task.
Task	The name of the task that triggered the audit log.
Timestamp	Time is UTC time in database that is mapped to the local time zone of client computer.
Result	The execution result of the task that triggered the audit log: <ul style="list-style-type: none"> • Success—Job completed successfully • Failure—Job failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started.
Job ID	For each job-based task, the audit log includes the job ID.
Description	A description of the audit log.

For both recurring and non-recurring jobs, such as a database backup, the Audit Logs table displays the following data described in [Table 81 on page 533](#).

Table 81: Audit Log Table Details for Recurring and Non-recurring Jobs

Field	Description
Job ID	The numerical ID of the job.
Percent	Percentage of job that has completed.
State	State of job execution: <ul style="list-style-type: none"> • SUCCESS—Job completed successfully • FAILURE—Job failed and was terminated. • IN PROGRESS—Job is in progress. • CANCELED—Job was canceled by a user.
Job Type	The supported job types. Job types depend on the installed Junos Space applications. In Junos Space 1.4, a recurring job type supported is Backup Database.
Summary	The operations executed for the job.
Scheduled Start Time	The scheduled start time for the job (specified by a Junos Space user).
Recurrence	The job recurrence interval, start time, and end time.

- Related Documentation**
- [Exporting Audit Logs on page 543](#)
 - [Viewing Audit Log Statistics on page 534](#)
 - [Junos Space Audit Logs Overview on page 531](#)
 - [Archiving and Purging Audit Logs on page 539](#)
 - [Junos Space User Interface Overview on page 9](#)
 - [Backing Up the Junos Space Network Management Platform Database on page 605](#)

Viewing Audit Log Statistics

The Audit log workspace statistics page provides two graphs: Audit Log Statistical Graph pie chart and the Top 10 Active Users in 24 Hours for the audit log administrator to monitor Junos Space Network Management Platform tasks.

The Audit Log Statistical Graph pie chart displays all tasks that have been performed and logged in all Junos Space applications over a specific period of time. You can view Audit Log statistics by task type, user, workspace, and application.



NOTE: Audit Logging is not currently supported by the Ethernet Design application. From Network Management Platform 12.1 onward, audit logging is supported by Service Now.

The Top 10 Active Users in 24 hours graph displays the top 10 Junos Space Network Management Platform users who have performed the most tasks over 24 hours. The graph X axis represents the activities performed by a single user. Each active session for that user is represented by a bubble on the X axis. The graph Y axis represents hours. For example, if a single user performed six active sessions during the last 24 hours, the chart displays six bubbles on the X axis according to the hours on the Y axis.

Viewing the Dynamic Audit Log Statistical Graph

The Audit Log Statistical Graph is an interactive graph that allows the audit log administrator to view audit logs by selecting both category and time frame. The category determines the statistical graph that displays—task, user, workarea, or application. Each slice in the pie represents a task and its usage percentage of the whole. The tasks types also appear in a list box at the right of the pie chart. Mousing over a slice of the pie displays the number of times the task is invoked. The time frame specifies the period of time within which to show audit log data.

To use the Audit Log Statistical Graph:

1. Select a graph category:

- Task—shows all tasks that have been performed. Click each task slice to go to the next level chart showing the users who performed the selected task.

The graph path displays the path to show where you are located in the UI. Click Overview to go back to the top level chart. The task name in the path indicates the currently selected path.

Tasks display in terms of user name or IP address.

- User names display all users by name. Click a user to go to the inventory page filtered by task, user, and selected time frame.
- IP address displays all IP address where users performed tasks. Click an IP address to go to the inventory page filtered by task, IP address, and selected time frame.
- Users displays all users using the system within the time frame. 10 users display per chart. Click Others to go to the next page. Click the previous page link to go back.
- Workspace displays all workspaces used in the time frame. Click a workspace slice to go to the inventory page filtered by workspaces.
- Application displays all applications used. Click a pie slice to go to the inventory page filtered by application and selected time frame.

2. Select a time frame in days, weeks, or months to display audit log data in the pie chart. The default is Days. A time selection description displays just below the time frame area.

- Days—Days mode displays the past seven days to the selected date. Select single or multiple days. Select multiple days by dragging the mouse
- Weeks—Weeks mode displays the past five weeks, from past to most current on the right.
- Months—Months mode displays the past 12 month, from past to most current on the right.

The current day, week, or month is highlighted.

3. Click a slice in the pie chart to view more detailed information. Tasks appear in tabular view by user name, user IP, task, timestamp, results, description, job ID, and level 2 description.

See [“Junos Space User Interface Overview” on page 9](#) for more information about manipulating the table data.

4. On the inventory page, click an audit log to view more detailed information. For a job-related log entry, there is a column for job-id, by clicking this link you will be led to a new table showing the corresponding Job info.

In the audit log detail view, if there are multiple affected objects for the log entry, the affected object detail always shows the first object detail. Clicking on any object in the list changes the object detail accordingly. If there is no affected object for this log entry, the affected object list is hidden and the object detail part is shown none.

5. Click Return to Audit Logs to go back to Audit Log View.

Viewing the Top 10 Active Users In 24 Hours Statistics

To view the Top 10 Active Users in 24 Hours graph:

1. In the Top 10 Active Users in 24 Hours graph, double-click a user's bubble for a particular hour. The View Audit Log page appears with the jobs performed by that user.

Tasks appear by user name, user IP, task, timestamp, results, description, job ID, and level 2 description in tabular view. See [“Junos Space User Interface Overview” on page 9](#) for more information about manipulating the table data.

Related Documentation

- [Viewing Audit Logs on page 532](#)
- [Junos Space Audit Logs Overview on page 531](#)
- [Junos Space User Interface Overview on page 9](#)
- [Archiving and Purging Audit Logs on page 539](#)
- [Exporting Audit Logs on page 543](#)

Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel

You can unzip an audit log *.gz file. You can open the extracted *.csv file as a spreadsheet in Microsoft Excel. In Microsoft Excel, you can convert the Coordinated Universal Time (UTC) timestamp column entries to local time.

To convert the UTC time to local time:

1. Retrieve the `JunosSpaceAuditLog_date_time_id.csv.gz` audit log file from where you archived it. If you archived the file locally, the file is located in `/var/lib/mysql/archive`.
 - Where *date* specifies the year, month, and day, in yyyy-mm-dd format
 - Where *time* specifies military, 24-hour time in hour, minutes, and seconds (hh-mm-ss) format
 - Where *id* is an auto-generated, 13-character random number that uniquely identifies each audit log archive file

For example, JunosSpaceAuditLog_2010-03-04-00-00-00_xx...x.csv.gz.

2. Unzip the audit log *.csv file.
3. Open the audit log *.csv file in Microsoft Excel.
4. To the left of the UTC Time column, insert a new column.
5. Label the column header **Local Time**.
6. Click the first cell of the new column.
7. Insert the following function: $=XX/86400000 + 25569 - X/24$
 - Where XX is the cell letter and row number where you want to insert the local time conversion function.
 - Where X represents the hours difference between your local time and the UTC time; divided by 24 hours.
8. Click Enter. The calculated local time appears.
9. Format the local time. Right-click the cell and select **Format Cells**. The Format Cells dialog box appears.
10. In the Category list box, select **Date**.
11. In the Type list box, select a date format that you want.
12. Click OK. The local time and date appears.
13. Copy or apply the cell function and formatting to the rest of the rows in the Local Time column. The rest of the local times appear as shown.

Figure 24: Formatting the Local Times Column in Microsoft Excel

	A	B	C	D	E	F	G	H	I	J
1	ID	Version	Timestamp	Local Time	UTC Time	User IP	Application	Task	Result	Correlation Tag
2	1900817	0	1.26971E+12	3/27/10 12:58	40264.70696	10.150.113.211	Network Application Platform	Archive/Purge	Job Scheduled	81E07BEDEF597C8CA5ECCEB14347FA29
3	1900821	0	1.26971E+12	3/27/10 13:14	40264.71815	10.150.113.211	Network Application Platform	Logout	Success	\N
4	1966342	0	1.26971E+12	3/27/10 13:24	40264.72546	10.150.113.211	Network Application Platform	Login	Success	\N
5										

14. If you want to keep the original audit log file, save it as a different filename.

Related Documentation

- [Archiving and Purging Audit Logs on page 539](#)

Archive / Purge

- [Archiving and Purging Audit Logs on page 539](#)

Archiving and Purging Audit Logs

The administrator can archive and then purge all audit logs files up to a specified data and time from the Junos Space Network Management Platform database. The administrator can archive audit logs to the local server or a remote server location.

The Junos Space Network Management Platform archive file uses the following naming conventions:

JunosSpaceAuditLog_date_time_id.csv.gz, where *date* specifies the year, month, and day, in the format **yyyy-mm-dd**, *time* specifies hours, minutes, and seconds, in the format **hh-mm-ss**, and *id* is a 13 character random number that uniquely identifies each audit log archive file.

This topic includes the following tasks:

- [Archiving Audit Logs To a Local Server and Purging the Database on page 539](#)
- [Archiving Audit Logs To a Remote Server and Purging the Database on page 540](#)

Archiving Audit Logs To a Local Server and Purging the Database

You can archive audit logs to the local server. The local server is the server that functions as the active node in the Junos Space fabric.

To archive Junos Space Network Management Platform audit log files to the local server and then purge the audit logs from the database:

1. Select **Audit Logs > Audit Log** and select the Archive/Purge Logs icon. The Archive/Purge dialog box appears.
2. In the Archive Logs Before field, specify the date and time up which to archived and purged audit logs from the Junos Space Network Management Platform database. You can only specify a date and time in the past.



NOTE: If you do not specify a date and time in the Archive Logs Before field, Junos Space Network Management Platform archives then purges from the database all logs generated up to the time that you initiated the operation.

3. In the Archive Mode field, select **local** from the list.
4. Schedule the Junos Space Network Management Platform Archive/Purge operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the Archive/Purge operation when you complete this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the Archive/Purge operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

5. Click **Submit**.

The Audit Log Archive and Purge confirmation dialog box displays the audit log file name and the location where it will be saved.
6. Click **Continue** to archive and purge the audit logs.
7. To view job details for the Audit Log Archive/Purge operation, click on the Job Id in the Job Information dialog box; otherwise, click **OK** to close the dialog box.

Archiving Audit Logs To a Remote Server and Purging the Database

You can archive audit logs to remote network hosts or media.

To back up the Junos Space Network Management Platform database to a remote host and then purge those logs from the Junos Space Network Management Platform database:

1. Select **Audit Logs > Audit Log** and select the Archive/Purge Logs icon. The Archive/Purge dialog box appears.
2. In the Archive Logs Before field, select a date and time to specify the date *up to which* all audit logs are to be archived and then purged from the Junos Space Network Management Platform database. You can only specify date and time in the past.



NOTE: If you do not specify a date and time in the Archive Logs Before field, Junos Space Network Management Platform will archive and then purge from the database all logs generated up to the time that you initiated the operation.

3. In the Archive Mode field, select **Remote** from the list.

4. Enter a valid user name to access the remote host server.
5. Enter a valid password to access the remote host server.
6. Reenter the password you entered in the previous step.
7. Enter the IP address of the remote host server.
8. Enter a directory path on the remote host server for the archived log files.



NOTE: The directory path must already exist on the remote host server.

9. Schedule the Junos Space Network Management Platform archive and purge operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the Archive/Purge operation when you complete this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the Archive/Purge operation.



NOTE: The selected time in the scheduler corresponds to Junos Space Network Management Platform server time but using the local time zone of the client computer.

10. Click **Submit**.

The Audit Log Archive and Purge dialog box displays the audit log file location and name and the remote server to which the files copy.

11. Click **Continue** to archive and purge the audit logs.

Junos Space Network Management Platform displays the Audit Log Archive and Purge Job Information dialog box.

12. To view job details for the Archive/Purge operation, click the Job Id link.
13. Click **OK** to close the dialog box.

Related Documentation

- [Junos Space Audit Logs Overview on page 531](#)
- [Viewing Audit Logs on page 532](#)
- [Exporting Audit Logs on page 543](#)

Export

- [Exporting Audit Logs on page 543](#)

Exporting Audit Logs

You can export audit logs without purging them from the system.

There are three options for this:

- Export all audit logs
- Export audit logs filtered by date range
- Export audit logs as displayed on View Audit Logs table. On the View Audit Logs page, you can filter audit logs according to multiple criteria. The criteria you choose determine which audit log data will be exported. The filter determines which records appear in the table, and all the records in the table will be exported.

The audit logs are exported as CSV files. They are not removed from the database when they are exported.

1. Select **Audit Logs > Audit Log**.

The Audit Log Statistical Graph page appears.

2. Select **Audit Logs > Audit Log** and select the Archive/Purge Logs icon. The Archive/Purge dialog box appears.
3. From the Audit Log Statistical Graph page, select a time period and category: Task, User, Workspace, or Application.
4. Click the graph to view the filtered audit logs
5. Click the **Export** link at the top of the table and below the title bar.

The **Export Audit Log** page appears.

6. Select one of the following options and click **Export**.

- **Export all audit logs.**

The Date and Time selectors are disabled when you choose this option.

- **Export audit logs filtered by date range .**

The Date and Time widget selectors are enabled when you choose this option.

- **Export audit logs as displayed on View Audit Logs table**

This is the default selection. For instructions on how to filter the logs, see [“Viewing Audit Logs” on page 532](#).

Your browser’s Download dialog appears.

7. You can choose to open the exported file or to save it.

**Related
Documentation**

- [Junos Space Audit Logs Overview on page 531](#)
- [Viewing Audit Log Statistics on page 534](#)
- [Archiving and Purging Audit Logs on page 539](#)

PART 12

Administration

- [Overview on page 547](#)
- [Fabric on page 551](#)
- [Managing Databases on page 603](#)
- [Manage Licenses on page 617](#)
- [Manage Applications on page 621](#)
- [Troubleshoot Space on page 647](#)
- [Manage Certificates on page 657](#)
- [Manage Authentication Servers on page 667](#)
- [Manage SMTP Servers on page 683](#)
- [Manage Tags on page 687](#)
- [Manage Permission Labels on page 701](#)
- [Manage DMI Schemas on page 713](#)
- [Generate Key on page 725](#)

CHAPTER 60

Overview

- [Junos Space Administrators Overview on page 547](#)
- [Maintenance Mode Overview on page 548](#)

Junos Space Administrators Overview

Junos Space administrators can serve different functional roles. A CLI administrator installs and configures Junos Space Appliances. A maintenance-mode administrator performs system-level tasks, such as troubleshooting and database restore operations. After appliances are installed and configured, users are created from the Junos Space user interface to access workspaces and manage applications, users, devices, services, customers, and so forth.

[Table 82 on page 547](#) shows the Junos Space administrators and the tasks that can be performed.

Table 82: Junos Space Administrators

Junos Space Administrator Function	Description	Tasks
CLI administrator	<p>An administrator responsible for setting up and managing system settings for Junos Space Appliances from the serial console.</p> <p>The CLI administrator name is “admin”.</p> <p>The CLI administrator password can be changed from the console system settings menu.</p>	<ul style="list-style-type: none">• Install and configure basic settings for Junos Space Appliances.• Change network and system settings for appliances, for example:<ul style="list-style-type: none">• Change CLI administrator password.• Set routing• Set DNS servers• Change time options• Expand VM drive size (Junos Space Virtual Appliances only)• Retrieve log files for troubleshooting

Table 82: Junos Space Administrators (*continued*)

Maintenance mode administrator	<p>An administrator responsible for performing system-level maintenance on Junos Space Network Management Platform.</p> <p>The maintenance mode administrator name is "maintenance".</p> <p>The maintenance mode password is configured from the serial console when you first configure a Junos Space Appliance.</p>	<ul style="list-style-type: none"> • Restore Junos Space Network Management Platform to previous state by using a database backup file. • Shut down Junos Space nodes by entering maintenance mode. • Retrieve log files for troubleshooting. • Exit Maintenance mode and explicitly start up Junos Space system.
Junos Space user interface users	<p>A Junos Space user that is assigned one or more predefined roles. Each role assigned to a user provides specific access and management privileges on the objects (applications, devices, users, jobs, services, customers) available from a workspace in the Junos Space user interface.</p>	<p>For complete information about the predefined roles that can be assigned to a Junos Space user, see "Predefined Roles Overview" on page 481.</p>

- Related Documentation**
- [Maintenance Mode Overview on page 548](#)
 - [Role-Based Access Control Overview on page 479](#)
 - [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)

Maintenance Mode Overview

In Junos Space Network Management Platform, *Maintenance mode* is a special mode that the administrator uses to perform database restore or debugging tasks while all nodes in the fabric are shutdown and the Junos Space Network Management Platform web proxy is running.

The Junos Space system goes into Maintenance mode in the following cases:

- Junos Space Network Management Platform goes down.

The system will go into Maintenance mode when Junos Space Network Management Platform is down on all nodes in the fabric. Users attempting to log in when the system is in Maintenance mode are redirected to the maintenance mode log in screen. Users who logged in to Junos Space Network Management Platform before the shutdown and attempt to perform an action in the user interface are also redirected to the maintenance mode log in screen.
- An authorized Junos Space administrator initiates a Restore Database from the Database Backup and Restore workspace.

When a user initiates a Restore database action, Junos Space Network Management Platform prompts the user for user name and password to enter maintenance mode, as shown in the Authentication Required dialog box. After the user is authenticated, Junos Space Network Management Platform initiates the restore database operation

and the system remains in Maintenance mode until the database is restored and the user exits maintenance mode.

- An authorized Junos Space administrator upgrades the Junos Space Network Management Platform software.

When a user initiates a software upgrade, Junos Space Network Management Platform prompts the user for user name and password to enter maintenance mode, as shown in the Authentication Required dialog box. After the user is authenticated, Junos Space Network Management Platform initiates the software upgrade and the system remains in Maintenance mode until the upgrade is finished and the user exits maintenance mode.

When a user is authenticated to access Junos Space Network Management Platform in maintenance mode, the Maintenance Mode Actions menu displays the tasks a user can perform in Maintenance Mode.

When a user exits maintenance mode, Junos Space Network Management Platform is restarted. After several minutes, the system returns to normal operational mode, and Junos Space users can log in to the user interface.

Maintenance Mode Access and System Locking

An authorized Junos Space administrator puts the system into maintenance mode by initiating a Restore database action.

Only one Maintenance mode administrator can access Maintenance mode at a time. When an administrator logs in to Maintenance mode, Junos Space Network Management Platform locks the page. When a second administrator attempts to log in to Maintenance mode while the first administrator is logged in, Junos Space Network Management Platform displays a message indicating that another administrator is currently logged in to the system and that Maintenance Mode is locked. The Maintenance mode lock releases when the first administrator logs out or the lock times out. If the logged-in administrator is inactive, the maintenance mode lock is released after 5 minutes at which time another administrator can log in.

Maintenance Mode User Administration

The user name for the maintenance mode administrator is “maintenance”.

The password for the maintenance mode administrator is set from the Junos Space system console during the initial installation/configuration of a Junos Space Appliance or Junos Space Virtual Appliance.

A Junos Space administrator connects to an appliance that is already in maintenance mode by using the URL `https://ip-address/maintenance`, where *ip-address* is the Web access IP address for the appliance.

Related Documentation

- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 610](#)
- [Backing Up the Junos Space Network Management Platform Database on page 605](#)
- [Backing Up and Restoring the Database Overview on page 604](#)

CHAPTER 61

Fabric

- [Fabric Management on page 551](#)

Fabric Management

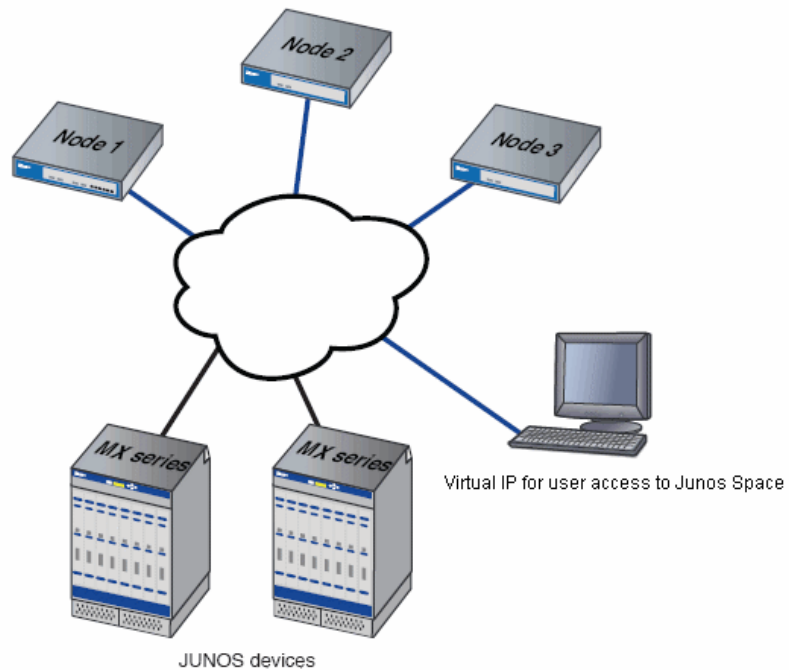
- [Fabric Management Overview on page 551](#)
- [Adding a Node to an Existing Fabric on page 556](#)
- [Viewing Nodes in the Fabric on page 557](#)
- [Configuring Node Network Settings on page 561](#)
- [Shutting Down or Rebooting a Node From Junos Space on page 566](#)
- [Deleting a Node on page 567](#)
- [Understanding Overall System Condition and Fabric Load on page 568](#)
- [Monitoring Nodes in the Fabric on page 570](#)
- [Creating a System Snapshot on page 598](#)
- [Deleting a System Snapshot on page 600](#)
- [Restoring the System to a Snapshot on page 600](#)

Fabric Management Overview

You can deploy a Junos Space Appliance or a Junos Space Virtual Appliance to create a fabric that provides the scalability and availability that your managed network requires as you add more devices, services, and users.

A Junos Space fabric comprises one or more IP-connected nodes. A *node* is a logical object that represents a single JA1500 Junos Space Appliance or Junos Space Virtual Appliance, its operating system, and the Junos Space Network Management Platform software that runs on the operating system. Each Junos Space Appliance or Junos Space Virtual Appliance that you install and configure is represented as a single node in the fabric. You can add nodes without disrupting the services that are running on the fabric. When you add nodes to the fabric, you can manage and monitor the nodes from the Administration workspace. To add, manage, and monitor nodes in the fabric, a fabric administrator connects to a single virtual IP address, as shown in the illustration.

Figure 25: Fabric Nodes



NOTE: All appliances (nodes) in a fabric must be from same Junos Space Network Management Platform release. For example, a fabric comprises Junos Space Release 1.1 appliances or Junos Space Release 1.2 appliances, but not both.

Single Node Functionality

When the fabric comprises a single appliance, all devices in the managed network connect to the appliance. When you install and configure the first appliance, Junos Space Network Management Platform automatically creates a fabric with one node. By default, a fabric that consists of a single node provides complete Junos Space Network Management Platform management functionality, with the following *node functions* enabled for the node:

- Load Balancer— for processing HTTP requests from remote browsers and NBI clients
- Database— for processing database requests (create, read, update, and delete operations)
- Application Logic— for processing back-end business logic (Junos Space Network Management Platform service requests) and DML workload (device connectivity, device events, and logging)



NOTE: A fabric that comprises a single node provides no workload balancing and no backup if the appliance goes down.

Multinode Functionality

As your network expands with new devices, services, and users, you can add Junos Space appliances to handle the increased workload. When you install and configure the first appliance, Junos Space Network Management Platform automatically creates a fabric with one node. For each additional appliance you install and configure, you must add a node to logically represent the appliance in the fabric. Each node that you add to the fabric increases the resource pool for the node functions to meet the scalability and availability requirements of your network. By default, Junos Space Network Management Platform automatically enables node functionality across the nodes in the fabric to distribute workload. The nodes in the fabric work together to provide a virtualized resource pool for each of the node functions: load balancer, database, and application logic.

The Junos Space Network Management Platform node functions distribute the workload across operating nodes according to the following load-distribution rules:

- **Load Balancer**— When a node that functions as the active load balancer server is down, all HTTP requests are automatically routed to the standby load balancer server that is running on a separate node.
- **Database**— When a node that functions as the active database server is down, all database requests (create, read, update, and delete) are routed to the node that functions as the standby database server.
- **Application Logic (DML and business logic)**— Device connections and user requests are distributed among the nodes, and device-related operations are routed to the node to which the device is connected.

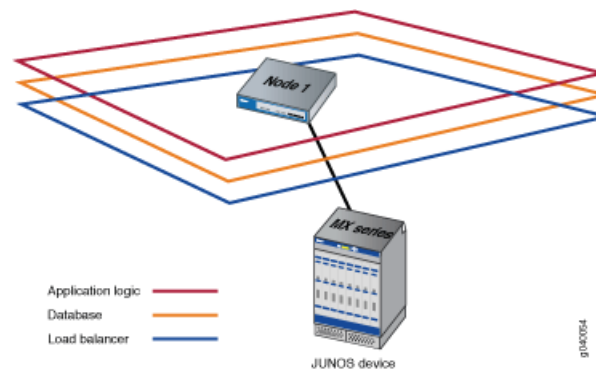
Junos Space Network Management Platform uses the following algorithm to ensure that the number of devices connected to a node does not exceed the threshold limit for each node:

$$\text{Threshold Limit} = [(\text{number of devices in database}) / (\text{number of nodes running})] + 2$$

The following workflow describes how the node functions are enabled across the fabric as nodes are added:

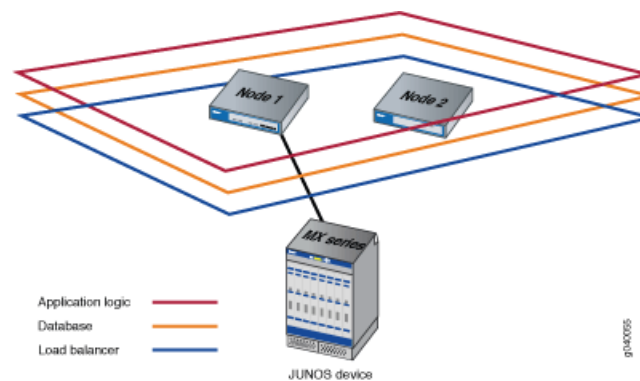
- **First node up:** The load balancer, database, and application logic functions are enabled on the node. Each node function provides both scalability and high availability. The following illustration shows all functions enabled on fabric comprising one node.

Figure 26: Fabric with One Node



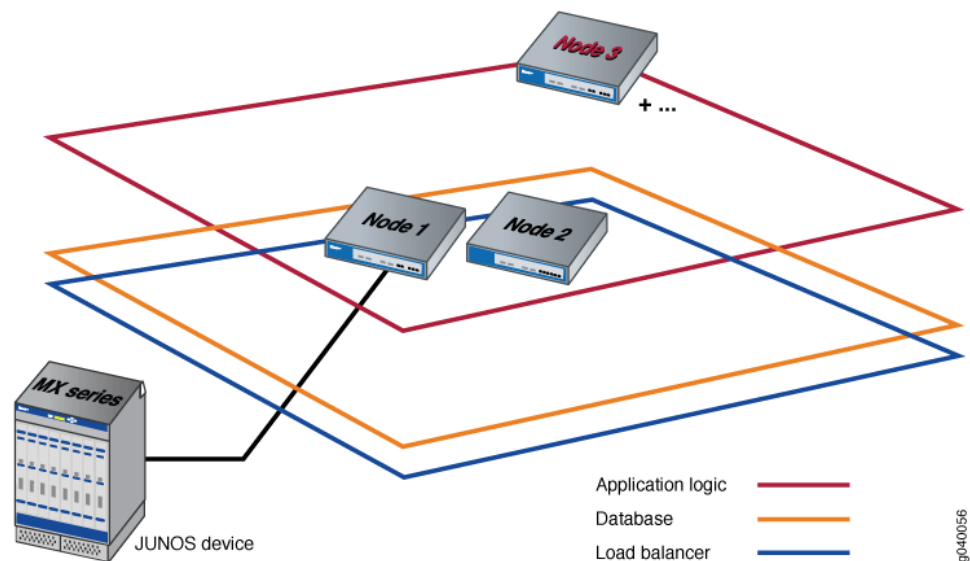
- Add second node: When a second node is added to the fabric, the first node functions as the active load balancer server and active database server, and the second node functions as the standby load balancer server and standby database server. The load balancer and application logic node functions provide scalability and high availability. The database node function on the second node provides high availability only. The following illustration shows the functions enabled on a fabric comprising two nodes.

Figure 27: Fabric with Two Nodes



- Add third node: Only the application logic functionality is enabled on the third node to provide equal distribution of device connections and user requests across all nodes, and route device-related operations to the node to which the device is connected. The application logic functionality provides both scalability and high availability. The following illustration shows the functions enabled on a fabric comprising three nodes.

Figure 28: Fabric with Three Nodes



NOTE: For the third node and each subsequent node added to the fabric, only the application logic functionality is enabled.

Node Function Availability

In a fabric comprising two or more nodes, Junos Space Network Management Platform provides failover when a node functioning as the active server (load balancer server or database server) goes down. By default, Junos Space Network Management Platform marks a particular node down and routes failover requests to the node that Junos Space Network Management Platform designates as standby server. Junos Space Network Management Platform uses a heartbeat mechanism to check whether the nodes in the fabric are running. When a node functioning as the active server fails (the appliance physically crashes or stops sending heartbeats), the node functioning as the standby server takes over all resources that were managed by the node functioning as active server.

Related Documentation

- [Viewing Nodes in the Fabric on page 557](#)

Adding a Node to an Existing Fabric

You can install one or more Junos Space appliances to create a scalable fabric. A Junos Space *appliance* can be either a JA1500 Junos Space Appliance or a Junos Space Virtual Appliance. Each Junos Space Appliance that you install is represented as a single node in the fabric. As the number of devices on your network expands, you can add nodes to the fabric to manage the increased workload. By default, the Junos Space fabric contains a single node that provides complete Junos Space Network Management Platform management functionality. When you install and configure the first appliance, Junos Space Network Management Platform automatically adds the first node to the fabric and uses the logical node name that you assign to the appliance when you configure the appliance in the command line interface. For each additional appliance that you install and configure, you must add the node in Junos Space Network Management Platform to represent the appliance in the fabric. You can add a maximum of six Junos Space nodes to the fabric including the first node.

Before you begin, the following prerequisites must be in place:

- Multicast needs to be enabled on the switches to which Space nodes are connected;
- IGMP-Snooping needs to be disabled on the switches to which Space nodes are connected. By default IGMP-snooping is enabled on most of the switches.
- All Junos Space nodes must be interconnected using a high-speed (1Gbps or 100Mbps) network with a maximum latency not to exceed 300 milliseconds.

To add a node to the Junos Space fabric:

1. Select **Network Management Platform > Administration > Fabric** and then select the **Add Fabric Node** icon.

The Add Fabric Node dialog box appears.



NOTE:

Before you add a node to the Junos Space fabric, verify the following:

- The installed image is identical to the images running on other nodes in the existing fabric.
 - During the initial configuration, the installer chose the option “yes” when prompted “Will this Junos Space system be added to an existing cluster?”
 - Ensure that no jobs are pending. No new jobs will be scheduled to run until the add node job has completed.
 - Also, if a Junos Space node that is part of an existing fabric is deleted, then you need to re-image the node before the node can be re-added to the fabric.
-

2. In the **Name** box, enter a name for the node.
3. In the **IP address** field, enter the IP address of the Junos Space Appliance.



NOTE: This is the IP address for interface eth0 that you specified during the basic configuration of the appliance.

4. (Optional) Schedule the Add Fabric Node operation:

- Clear the **Schedule at a later time** check box (the default) to initiate the add node operation when you complete step 5 of this procedure.
- Select the **Schedule at a later time** check box to specify a later start date and time for the add node operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but is mapped to the local time zone of the client computer.

5. Select **Add** to add the node to the fabric.

The node is added to the fabric and appears in the Junos Space user interface and database. When you add a node, the node functions are automatically assigned by Junos Space Network Management Platform.

By default, the first and second Junos Space nodes added to a fabric perform all the following functions:

- Database—For processing database requests (create, read, update, and delete operations)
- Load Balancer—For processing HTTP requests from remote browsers and NBI clients
- Application Logic—For processing back-end business logic (Junos Space Network Management Platform service requests), and DML workload (device connectivity, device events, and logging)

By default, the third Junos Space node, and all subsequent Junos Space nodes, added to a fabric perform only the Application Logic function. You can add a maximum of six Junos Space nodes to a fabric including the first node.

Related Documentation

- [Fabric Management Overview on page 551](#)
- [Viewing Nodes in the Fabric on page 557](#)
- [Overall System Condition and Fabric Load History Overview on page 568](#)

Viewing Nodes in the Fabric

The Fabric Monitoring inventory page allows the administrator to monitor each node in the Junos Space fabric. You can also monitor the status of the database, load balancer,

and application logic functions running on each node, and identify nodes that are overloaded or down. The Fabric inventory page refreshes every 10 seconds, by default.

- [Changing Views on page 558](#)
- [Viewing Fabric Node Details on page 558](#)
- [Performing Fabric Node Actions on page 560](#)

Changing Views

You can display fabric monitoring in a tabular view. The fabric nodes appear in a table sorted by node name. Each fabric is a row in the Fabric Monitoring table.

To change views:

1. Select **Administration > Fabric**. The **Fabric** page appears.
2. Click a view indicator at the left of the Fabric page title bar.

Viewing Fabric Node Details

To view detailed runtime and status information for a node:

- Double-click a node in the table view. The **View Node Detail** page appears.

[Table 83 on page 558](#) describes the node information displayed in each column in the table and from the detailed view.

Table 83: Fields for the Fabric Monitoring Inventory Page

Field	Description
Node name	<p>The logical name assigned to the node.</p> <p>NOTE: For the first node, Junos Space uses the node name that the user specifies during the initial configuration of the Junos Space Appliance (physical or virtual). For each subsequent node, the user must specify a node name when adding the node to the fabric.</p>
Management IP	The IP address for the node.
Device Connection IP	The IP address for connecting to the device.
Status	<p>Connection status for the node.</p> <ul style="list-style-type: none"> • UP—Node is connected to the fabric. • DOWN—Node is disconnected from the fabric.
% CPU	<p>The percentage of CPU resource utilized by the node; from 0 to 100%.</p> <ul style="list-style-type: none"> • Unknown—The percentage of CPU utilized is unknown, for example, because the node is not connected.

Table 83: Fields for the Fabric Monitoring Inventory Page (*continued*)

Field	Description
% Memory	<p>The percentage of memory resource utilized by the node; from 0 to 100%.</p> <ul style="list-style-type: none"> Unknown—The percentage of memory utilized is unknown, for example, because the node is not connected.
% DISK	<p>The percentage of the /var directory utilized by the node; from 0 to 100%.</p> <ul style="list-style-type: none"> Unknown—The percentage of the /var directory utilized by the node is unknown, for example, because the node is not connected.
App Logic	<p>Application logic function status for the node.</p> <ul style="list-style-type: none"> UP— Application logic function is running on node. DOWN—Application logic function enabled on the node but is not running. Unknown—Status for the application logic function is unknown, for example, because the node is not connected. N/A— Application logic function is not configured to run on the node. (Master)—The configured primary Junos Space node in the fabric.
Database	<p>Database function status for the node.</p> <ul style="list-style-type: none"> UP—Database function is running on node. DOWN—Database function that is enabled on the node but is not running. Unknown—Status for the database function is unknown, for example, because the node is not connected. N/A—Database function is not configured to run on the node. <p>NOTE: By default, the database function is enabled on no more than two nodes in the fabric.</p>
Load balancer	<p>Load balancer function for the node.</p> <ul style="list-style-type: none"> UP – Load balancer function is running on the node. DOWN – Load balancer function that is enabled on the node is not running. Unknown – Status for the Load balancer function is unknown, for example, because the node might not be connected. N/A – Load balancer function is not running because it is not configured to run on the node. <p>NOTE: By default, the Load balancer function is enabled on no more than two nodes in the fabric.</p> <ul style="list-style-type: none"> (VIP)—The configured virtual IP node in the fabric.
Hardware model	<p>Model of Junos Space Appliance. For example, this field can have values, such as “JA1500,” “VMware Virtual Platform,” and so on.</p> <p>NOTE: Hardware model appears when you double-click table row for a detailed view of the node.</p> <p>NOTE: Hardware model only applies for a physical Junos Space Appliance.</p>

Table 83: Fields for the Fabric Monitoring Inventory Page (*continued*)

Field	Description
Software version	Junos Space Network Management Platform Release Version. NOTE: Software version appears when you double-click a table row for a detailed view of the node.
Serial number	Serial number for the Junos Space Appliance. NOTE: Serial number appears when you double-click a table row for a detailed view of the node.
Cluster Member IPs	The IP addresses of the nodes in the fabric.
Is Master Node	Indicates whether node is master node. <ul style="list-style-type: none"> • TRUE—Node is master node. • FALSE—Node is not master node.
Is VIP Node	Indicates whether node is a virtual IP (VIP) node. The first (active) node and second (standby) node are VIP nodes. <ul style="list-style-type: none"> • TRUE—Node is VIP node. • FALSE—Node is not VIP node.

For more information about manipulating data on the Fabric inventory page, see [“Junos Space User Interface Overview” on page 9](#).

Performing Fabric Node Actions

To perform an action:

- Select a node by clicking the check box adjacent to the node on the Fabric page.
- Select an action from the Actions menu.

From the Fabric inventory page, you can perform the following actions:

- **Shut Down Node**—Shuts down or reboots fabric nodes (appliances or virtual machine hosts) when you move them or reconfigure their network settings. See [“Shutting Down or Rebooting a Junos Space Appliance Node From Junos Space” on page 566](#).
- **Delete Fabric Node**—Removes node from the Junos Space fabric directly, if there is a physical or virtual appliance failure. See [“Deleting a Node from the Junos Space Fabric” on page 567](#).
- **ESX Configuration**—Perform ESX server configuration.

If you want to take a snapshot of a Junos Space server running on a VM within an ESX server, then it is necessary that you provide the ESX server information.

- **SNMP Configuration**—Perform SNMP configuration. Junos Space Network Management Platform supports SNMP monitoring by an SNMP manager for SNMP v1, v2c, and v3.

- **SNMP Start**—Start monitoring a node.
- **SNMP Stop**—Stop monitoring a node.
- **SNMP Restart**—Restart monitoring a node.
- **Delete Private Tags**—Delete private tags (that is, the tags you created).
- **Tag It**—Apply a tag to a fabric node. See [“Tagging an Object” on page 695](#).
- **View Tags**—View tags applied to a fabric node. See [“Viewing Tags for a Managed Object” on page 696](#).
- **Untag It**—Remove a tag from a fabric node. See [“Untagging Objects” on page 697](#).
- **Clear All Selections**—Clears the selection from all objects selected on the inventory page.

Related Documentation

- [Overall System Condition and Fabric Load History Overview on page 568](#)
- [Fabric Management Overview on page 551](#)
- [Junos Space User Interface Overview on page 9](#)

Configuring Node Network Settings

The Junos Space fabric consists of one or multiple nodes. Network settings for these nodes enable IP connectivity to external systems as well as internal connectivity between nodes. During the initial set up of a node, the Junos Space super administrator configures node networking settings through the CLI interface. However, you cannot use the CLI interface to change network settings.

To change fabric node settings, navigate to **Network Management Platform > Administration > Fabric > Space Node Settings**. Changing node settings allow you to move Junos Space fabric from one network location to another location without reinstallation.

Existing settings for both the management interface and device management interface (IP address, net mask and default gateway) for all nodes are displayed in a table. The settings for a node are displayed as a row in the table.

Nodes require restart to apply new network settings.

This topic includes the following topics:

- [Network Settings Configuration Guidelines on page 562](#)
- [Changing the VIP Interface in the Same Subnet on page 562](#)
- [Changing the Node Management IP in the Same Subnet on page 562](#)
- [Changing the Default Gateway on page 562](#)
- [Changing the Management IP to a Different Network on page 563](#)
- [Adding the Device Management IP Address on page 563](#)
- [Changing the Device Management IP Address in the Same Subnet on page 564](#)
- [Changing the Device Management IP Address to a Different Network on page 564](#)

- [Deleting a Device Management IP Address on page 564](#)
- [Changing the VIP Interface to a Different Network on page 565](#)
- [Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet on page 565](#)
- [Changing the VIP interface of a Multi-Node Fabric to a Different Network on page 565](#)

Network Settings Configuration Guidelines

- The virtual IP (VIP) interface and Node IP address should be in the same subnet.
- The node management IP address of the first two nodes in the fabric must be in the same subnet.
- When you modify the device management IP address, all the devices connected to that node should be updated with the new device management IP address.

Changing the VIP Interface in the Same Subnet

There is only one VIP for the entire fabric.

Changing the Node Management IP in the Same Subnet

To change the node management IP in the same subnet:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to change the management IP.
The settings appear for you to modify
3. Change the management IP in the same subnet.
4. Click **OK**.
5. Click **Modify**.
The Shutdown/reboot confirmation dialog box appears.

Changing the Default Gateway

To change the default gateway:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to change the default gateway.
The settings appear for you to modify
3. Change the default gateway.
4. Click **OK**.
5. Click **Modify**.
The Shutdown/reboot confirmation dialog box appears.

Changing the Management IP to a Different Network

To change the management IP to a different network:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to change the management IP.
The settings appear for you to modify.
3. Change the management IP from a different network.
4. Change the VIP, subnet mask, and default gateway.
5. Click **OK**.
6. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Adding the Device Management IP Address



NOTE: On a Junos Space fabric with two or more Junos Space nodes, if you configure the eth3 interface as the device management interface on one Junos Space node, then you must also configure the eth3 interface as the device management interface on all the other Junos Space nodes in that fabric.

To add the device management IP address:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to add the device management IP address.
The settings appear for you to modify.
3. Select **Enable Device Interface**.
4. Add the VIP, subnet mask, and default gateway for the device management interface.
5. Click **OK**.
6. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Changing the Device Management IP Address in the Same Subnet

To change the device management IP address in the same subnet:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to change the device management IP.

The settings appear for you to modify.

3. Change the device management IP to a new one in the same subnet.
4. Click **OK**.
5. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Changing the Device Management IP Address to a Different Network

To change the device management IP address to a different network:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to change the device management IP.

The settings appear for you to modify.

3. Change the device management IP to a new one in a different subnet.
4. Change the subnet mask and default gateway.
5. Click **OK**.
6. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Deleting a Device Management IP Address

To delete a device management IP address

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to delete the device management IP address.

The settings appear for you to modify.

3. Clear the **Enable Device Interface** check box.
4. Click **OK**.
5. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Changing the VIP Interface to a Different Network

The VIP interface and the node IP should be in the same subnet.

To change the VIP interface to a different network:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Change the VIP interface to a different network.
3. Change the node IP address.
4. Click **OK**.
5. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet

To change the node management IP address and all nodes in the fabric to the same subnet:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Click the pencil icon for the node on which you want to change the node management IP address.

The settings appear for you to modify.

3. Change the node management IP address to a new one in the same subnet.
4. Click **OK**.
5. Repeat Steps 1 through 3 for each node in the fabric.
6. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

Changing the VIP interface of a Multi-Node Fabric to a Different Network

The node IP address and the VIP interface must be in the same subnet.

To change the VIP interface of a multi-node fabric to a different network:

1. Select **Administration > Fabric > Space Node Settings**. The Space Node Settings page appears.
2. Change the VIP interface to a new one in a different network.
3. Change the node IP address.

4. Click **OK**.
5. Repeat Steps 1 through 3 for each node in the fabric.
6. Click **Modify**.

The Shutdown/reboot confirmation dialog box appears.

**Related
Documentation**

- [Shutting Down or Rebooting a Junos Space Appliance Node From Junos Space on page 566](#)

Shutting Down or Rebooting a Node From Junos Space

From Junos Space Network Management Platform, the super administrator can shut down or reboot fabric nodes (appliances or virtual machine hosts) when they are moved or their network settings reconfigured. You can shut down or reboot a fabric node using the **Network Management Platform > Administration > Shut Down Node** action. Optionally, you can enter a message to display to administrators logged in to an affected node.

To shut down or reboot a node in the fabric,

1. Select **Administration > Fabric**. The Fabric page appears.
2. Select the nodes.
3. Select **Shutdown Node** from the Actions menu.

The **Reboot Node/Shutdown Node** dialog box appears.

4. Select the appropriate action by clicking either the **Shutdown** or the **Reboot** option.
5. (Optional) You can enter a message to be displayed to console users (for any administrator logged into the node using the CLI. The message appears on UNIX shell).

If you do not enter anything, console users will see either **Junos Space shutdown** or **Junos Space reboot** on the shell.

6. Click **Confirm**.

The shut down or reboot action occurs.



NOTE: If you are shutting down a node after a change of IP address, it is recommended that you reboot all the nodes for the changes to take effect.

**Related
Documentation**

- [Fabric Management Overview on page 551](#)
- [Deleting a Node from the Junos Space Fabric on page 567](#)
- [Viewing Nodes in the Fabric on page 557](#)

Deleting a Node

You can delete a node from the Junos Space fabric directly by selecting the node and selecting **Delete Fabric Node** from the Actions menu. You must remove the deleted node from the network and re-image it. Thereafter, you can add it to the fabric by selecting **Administration > Fabric** and the **Add Fabric Node** icon.

You can delete a node from the fabric under the following conditions:

- In a multiple node fabric if that node does not disrupt activities of other nodes.
- If a node is configured for high availability—with load balancing and as a database server capability—and there is another node that has the capacity to assume that role. You are prompted to enable that role on another candidate node before deleting that node. If you delete a high availability node, but there is not another node to transfer that role, high availability does not occur.

When you delete a fabric node, Junos Space Network Management Platform does the following:

- Removes reference to that node host name and IP address from remaining nodes.
- Stops database replication on both the deleted node and the backup database node.
- The database backup copy in that node will not be available for the remaining cluster to restore from that copy.
- Copies the database to the new database node.
- Shuts down all services that interact with other nodes.

You can delete only one node at a time. You must have Super Administrator or System Administrative role access privileges to delete a node.

To delete a node:

1. Select **Administration > Fabric**.

Select the node that you want to delete, and select **Delete Fabric Node** from the Actions menu.

2. In the Warning dialog box, confirm that you want to delete the node by clicking **Continue**.

- If a node you want to delete is not configured for high availability or a node is configured for high availability but there is no other node available to assume that role, the **Delete Node** dialog box appears displaying the node name and management IP address of only the node you want to delete.
- If a node is configured for high availability, the **Delete Node** dialog box notifies you of that fact and lists all candidate nodes that have the capacity to take over that role.

3. In the **Delete** dialog box, select the node you want to delete.
4. Click **Delete**.

Node deletion is scheduled as a job immediately after you click **Delete**. The Delete Node action is also audit logged. The **Delete Fabric Node Job Information** dialog box appears.

5. In the **Delete Fabric Node Job Information** dialog box, click the **Job ID** link.

Job Manager displays the **View Job Details** dialog box for you to verify and monitor delete node information, such as job type, job ID, percent complete, job state, scheduled start and end time, user name, and a brief job summary.

6. If a problem occurs in the delete node job, you can troubleshoot by viewing the job status in the **Network Management Platform > Audit Logs > Audit Log** inventory page.



NOTE: When you delete a node, a UDP communication exception occurs. This behavior is normal.



NOTE: When you delete a load balancer node, a VIP switch may occur and cause the Junos Space Network Management Platform progress indicator to appear. This behavior is normal.

**Related
Documentation**

- [Fabric Management Overview on page 551](#)
- [Viewing Nodes in the Fabric on page 557](#)
- [Adding a Node to an Existing Junos Space Fabric on page 556](#)

Understanding Overall System Condition and Fabric Load

You can view the overall Junos Space system condition and fabric load from the Junos Space Network Management Platform application dashboard or from the Administration workspace landing page.

System Condition

To calculate the overall system condition, Junos Space Network Management Platform uses an algorithm based on cluster health and node-function health:

- Cluster health indicates the percentage of nodes in the fabric that are currently running.

For example, if only three nodes are reachable in a four-node fabric, cluster health is 75%.

- Load-balancer health indicates the percentage of nodes (enabled for load balancing) that are running the load balancing process.

For example, if two nodes are enabled for load balancing and the load-balancing process is running on only one node, the load-balancing health is 50%.

- Database health indicates the percentage of nodes (enabled for database requests) that are running the database process.

For example, if two nodes are enabled as database server and the database process is running on only one node, then database health is 50%.

- Application-logic health indicates the percentage of nodes (enabled for application logic (DML and business logic) that are running the application-logic process.

For example, if three nodes are enabled for application logic and the application-logic process is running on only two nodes, then application-logic health is 67%.

Junos Space Network Management Platform retrieves data on the nodes and the node functions running, and then applies the following algorithm to determine the overall system condition:

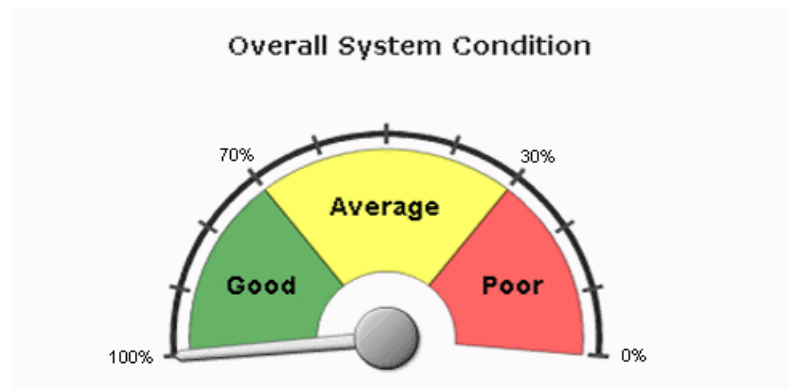
$$\text{overall system condition} = [(\text{number of nodes running}) / (\text{number of nodes in fabric})] * [(\text{number of nodes running load balancing process}) / (\text{number of nodes enabled for load balancing})] * [(\text{number of nodes running database server process}) / (\text{number of nodes enabled as database server})] * [(\text{number of nodes running application logic process}) / (\text{number of nodes enabled for application logic})]$$

Using the preceding examples for cluster health and node-function health, the overall system condition is expressed as a percentage:

$$\text{overall system condition} = 75\% * 50\% * 50\% * 67\% = 12.5\%$$

The Overall System Condition dialog box indicates Poor (0–30%), Average (30–70%), or Good (70–100%), based on the value the algorithm returns.

Figure 29: Overall System Condition Gauge



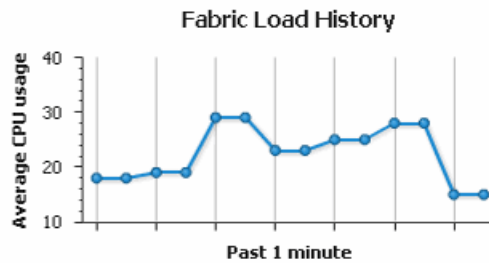
The overall system health indicates 0% (Poor) when any one of the following conditions is detected:

- No nodes in the fabric are running.
- No nodes enabled for load balancing are running the load balancing process.
- No nodes enabled for database requests are running the database process.
- No nodes enabled for application logic are running the application logic process.

Fabric Load

The Fabric Load chart displays the average CPU usage across all nodes that are running in the fabric.

Figure 30: Fabric Load History Chart



Junos Space Network Management Platform uses the following algorithm to determine the fabric load:

$$\text{fabric load} = [\text{total CPU usage for all nodes running}] / [\text{number of nodes running}]$$

For example, given a fabric with three nodes running and CPU usage of 80%, 30%, and 10%, respectively, the fabric load is 40%. The following example illustrates how the fabric load is calculated.

$$\begin{aligned} \text{fabric load} &= [80\% + 30\% + 10\%] / 3 \\ \text{fabric load} &= 120\% / 3 \\ \text{fabric load} &= 40\% \end{aligned}$$

To view the average CPU use at a specific data point, drag the mouse over the data point of interest.

To obtain details about the status of the fabric, click any data point in the graph. The Fabric dialog box appears and shows detailed status for each node in the fabric. Status information includes CPU, disk, and memory usage and indicates up or down status for each node function enabled on the node.

- Related Documentation**
- [Fabric Management Overview on page 551](#)
 - [Junos Space User Interface Overview on page 9](#)

Monitoring Nodes in the Fabric

As an administrator or operator, you can use Junos Space to track the status of logical components of deployed nodes in a fabric.

The Network Application Platform supports SNMP Monitoring by an SNMP Manager for SNMP v1, v2c, and v3.

The SNMP manager polls Space to get information about the logical components of the nodes using an object identifier (OID) in SNMP v1 and v2, or in v3 as a user. The response

is provided by the Space SNMP agent. The network monitoring functionality displays the polled data in the Network Monitoring workspace.

Every Space node in the fabric has an SNMP configuration file on the server at the location shown (`/etc/snmp/snmpd.conf`).

[Table 84 on page 571](#) shows the monitoring settings, as well as relevant details.

Table 84: Logical Component Monitoring

Setting	Explanation	Recommended Settings	Default Value	Comments
Enable SNMP over TCP	Enables Space to monitor itself over SNMP, which provides more detail than TCP.	Selected	Unselected	This is not set by default because self-monitoring impacts performance
Monitor Web Service	Includes monitoring the performance of the Space GUI.	Selected	Selected	
Monitor All Disks	Includes all disks on the current Space server.	Unselected	Unselected	All disks, or specify partition
Monitor RAID	Enables Net-SNMP to monitor the RAID state. When a RAID controller fault is detected, a trap is sent.	Selected	Selected	
Disk Usage %	When the percentage of the disk in use exceeds the number set here, an alarm is triggered.	5	5	
System Load (1 min)	When the system load exceeds the number set here, an alarm is triggered.	4	4	
System Load (5 min)	When the system load exceeds the number set here, an alarm is triggered.	4	4	
System Load (15 min)	When the system load exceeds the number set here, an alarm is triggered.	4	4	
System Location	Place where the system is located, for example, New York City.	Actual geographical or other location	unknown	

Table 84: Logical Component Monitoring (*continued*)

Setting	Explanation	Recommended Settings	Default Value	Comments
System Contact	E-mail address to which the system sends notifications.	E-mail address of actual person	root <root@localhost>	
Disk Mount Path	Path of the disk to be mounted.	Actual path, if available	/	
CPU Max Temp (mC)	When the temperature exceeds the number set here, an alarm is triggered.	50000	50000	
CPU Min Fan (RPM)	When the minimum fan speed exceeds the number set here, an alarm is triggered.	1000	1000	
CPU Min Voltage (mV)	When the minimum voltage exceeds the number set here, an alarm is triggered.	1000	1000	

- [Viewing and Modifying the SNMP Configuration for a Fabric Node on page 572](#)
- [Starting SNMP Monitoring on Fabric Nodes on page 594](#)
- [Stopping SNMP Monitoring on Fabric Nodes on page 595](#)
- [Restarting SNMP Monitoring on Fabric Nodes on page 595](#)
- [Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node on page 596](#)
- [Adding a Third-Party SNMP V3 Manager on a Fabric Node on page 596](#)
- [Deleting a Third-Party SNMP Manager from a Fabric Node on page 597](#)

Viewing and Modifying the SNMP Configuration for a Fabric Node

To view and edit the Space SNMP configuration for self-monitoring:

1. Select **Network Management Platform > Administration > Fabric**.

The Fabric page appears.

2. Select the node whose configuration you want to view or modify, and from the Actions menu, select **SNMP Configuration**.

The SNMP Configuration window appears with the title bar displaying the IP address of the selected node.

3. Set the SNMP configuration parameters as required, using [Table 84 on page 571](#) to guide you.



.....

NOTE: The System Load Threshold is set to 4, which indicates only alert when all CPUs are under 100 percent load.

.....

4. Select **Confirm** to apply the SNMP configuration changes to the node, or select **Cancel** if you do not want to make any changes to the SNMP configuration.

[Table 85 on page 574](#) shows the configuration parameters for monitoring disk usage.

Table 85: SNMP Configuration Parameters: Monitoring Disk Usage

Monitoring Disk Usage

Table 85: SNMP Configuration Parameters: Monitoring Disk Usage (*continued*)

Monitoring Disk Usage

Parameter: Disk Usage (%)

Default: 5%

When the free disk space is greater than the configured threshold, the trap shown in [Figure 31 on page 575](#) is generated.

Figure 31: Disk Usage Threshold Is Normal

	406	space-000c29d796f5	1	3/27/14 12:25:51 [<] [>]	Disk usage is normal.
---	-----	--------------------	---	--	-----------------------

[Figure 32 on page 575](#) shows the OID details for the trap generated when disk usage is normal.

Figure 32: Trap Details When Disk Usage Normal

Trap Details

Request ID: 1861140816
Community: public
Ip Address: 10.205.56.39
Trap Type: SNMPv2c
Error Index: 0
Error Status: 0

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.11s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	Disk space usage clear
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	String	
mib-2.88.2.1.5.0	OID	1.3.6.1.4.1.2021.9.1.100.1
diskPath.1	Integer	0
diskErrorMsg.1	String	/

Trap Details


Request ID: 1861140816
Community: public
Ip Address: 10.205.56.39
Trap Type: SNMPv2c
Error Index: 0
Error Status: 0

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.11s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Disk space usage clear
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	String	
1.3.6.1.2.1.88.2.1.5.0	OID	1.3.6.1.4.1.2021.9.1.100.1
1.3.6.1.2.1.88.2.1.5.0	Integer	0
1.3.6.1.4.1.2021.9.1.2.1	String	/
1.3.6.1.4.1.2021.9.1.101.1	String	

When the free disk space is less than the configured threshold, the trap shown in [Figure 33 on page 575](#) is generated.

Figure 33: Disk Usage Threshold Exceeds Configured Threshold

	377	space-000c29d796f5	2	3/27/14 11:59:48 [<] [>]	Disk usage threshold upper limit exceeded./: less than 95% free (= 63%).
---	-----	--------------------	---	--	--

[Figure 34 on page 575](#) shows the OID details for the trap generated when disk usage exceeds the configured threshold.

Figure 34: Trap Details When Disk Usage Exceeds Configured Threshold

Table 85: SNMP Configuration Parameters: Monitoring Disk Usage (*continued*)

Monitoring Disk Usage

Trap Details		
Request ID	1141303069	
Community	public	
Ip Address	10.205.56.39	
Error Index	0	
Error Status	0	
Trap Type	SNMPv2c	
Variable Bindings		
OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.11s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	Disk space usage trigger
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.9.1.100.1
mib-2.88.2.1.5.0	Integer	1
dskPath.1	String	/
dskErrorMsg.1	String	/: less than 90% free (= 25%)
<input type="button" value="Close"/> <input type="button" value="Show Raw"/> <input type="button" value="prev"/> <input type="button" value="next"/>		

Table 86 on page 577 shows the configuration parameters for monitoring the CPU load average.

Table 86: SNMP Configuration Parameters: Monitoring the CPU Load Average

Monitoring the CPU Load Average (System Load)

Table 86: SNMP Configuration Parameters: Monitoring the CPU Load Average (*continued*)

Monitoring the CPU Load Average (System Load)

Parameter: CPU Load (1 min, 5 min, 15 min)

Default Threshold Value: 4

When the CPU Load Average threshold is less than or equal to the configured threshold limit, the trap shown in Figure 35 on page 578 is generated:

Figure 35: CPU Load Average Threshold Is Normal

<input type="checkbox"/>	379	space-000c29d796f5	1	3/27/14 12:00:48 [<] [>]	CPU load average is normal.
--------------------------	-----	--------------------	---	--------------------------	-----------------------------

Figure 36 on page 578 shows the OID details for the trap generated when the CPU load is normal.

Figure 36: Trap Details When CPU Load Average Threshold Is Normal

Trap Details

Request ID: 1141303118
Community: public
Ip Address: 10.205.56.39
Error Index: 0
Error Status: 0
Trap Type: SNMPv2c

Variable Bindings:

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.12s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	CPU LA clear
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	String	
mib-2.88.2.1.5.0	Integer	0
laNames.3	String	Load-15
laErrorMessage.3	String	

Close Show Raw << prev next >>

Trap Details

Request ID: 1141303118
Community: public
Ip Address: 10.205.56.39
Error Index: 0
Error Status: 0
Trap Type: SNMPv2c

Variable Bindings:

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.12s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	CPU LA clear
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	String	
1.3.6.1.2.1.88.2.1.5.0	Integer	0
1.3.6.1.4.1.2021.10.1.2.3	String	Load-15
1.3.6.1.4.1.2021.10.1.101.3	String	

Close Show Raw << prev next >>

Figure 37 on page 578 shows the traps generated when the 15 minute, 5 minute, or 1 minute CPU Load Average threshold is exceeded.

Figure 37: CPU Load Average Threshold – Upper Limit Exceeded

<input type="checkbox"/>	368	space-000c29d796f5	3	3/27/14 11:59:49 [<] [>]	CPU load average threshold upper limit exceeded. 1 5 min Load Average too high (= 1.01).
<input type="checkbox"/>	362	space-000c29d796f5	3	3/27/14 11:59:48 [<] [>]	CPU load average threshold upper limit exceeded. 5 min Load Average too high (= 1.11).
<input type="checkbox"/>	360	space-000c29d796f5	4	3/27/14 11:59:48 [<] [>]	CPU load average threshold upper limit exceeded. 1 min Load Average too high (= 1.04).

Figure 38 on page 578 shows the OID details for the trap generated when the CPU load 5 minute average exceeds the threshold.

Figure 38: Trap Details When CPU Load 5 Minute Average Exceeds Threshold

Table 86: SNMP Configuration Parameters: Monitoring the CPU Load Average (*continued*)

Monitoring the CPU Load Average (System Load)

Trap Details

Request ID

1861140846

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.11s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	CPU LA trigger
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.10.1.100.2
mib-2.88.2.1.5.0	Integer	1
laName.2	String	Load-5
laErrorMessage.2	String	5 min Load Average too high (= 1.14)

Close

Show Raw

<< prev

next >>

Trap Details

Request ID

1861140846

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.11s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	CPU LA trigger
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.10.1.100.2
1.3.6.1.2.1.88.2.1.5.0	Integer	1
1.3.6.1.4.1.2021.10.1.2.2	String	Load-5
1.3.6.1.4.1.2021.10.1.101.2	String	5 min Load Average too high (= 1.14)

Close

Show Raw

<< prev

next >>

Table 87 on page 580 shows monitoring processes for the Junos Space Network Management Platform.


Table 87: SNMP Configuration Parameters: Monitoring Processes

Monitoring Processes

Parameter: Node Management Agent (NMA)

When the NMA process is up, the trap shown in [Figure 39 on page 580](#) is generated:

Figure 39: NMA Is Up

	384	space-000c29d796f5	1	3/27/14 12:10:05 [<] [>]	Process NMA started.
---	-----	--------------------	---	--------------------------	----------------------

[Figure 40 on page 580](#) shows the OID details for the trap generated when the NMA process is up.

Figure 40: Trap Details When NMA Is Up

Request ID

1861140004

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:00m:05.91s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	NMA started
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.2
mib-2.88.2.1.5.0	Integer	104
extNames.2	String	NMA
extOutput.2	String	

Close

Show Raw

<< prev

next >>

Request ID

1861140004

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:00m:05.91s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	NMA started
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.2
1.3.6.1.2.1.88.2.1.5.0	Integer	104
1.3.6.1.4.1.2021.8.1.2.2	String	NMA
1.3.6.1.4.1.2021.8.1.101.2	String	

Close


Show Raw

<< prev

next >>

When the NMA process is down, the trap shown in [Figure 41 on page 580](#) is generated:

Figure 41: NMA is Down

	382	space-000c29d796f5	1	3/27/14 12:09:25 [<] [>]	Process NMA stopped.
---	-----	--------------------	---	--------------------------	----------------------

[Figure 42 on page 580](#) shows the OID details for the trap generated when the NMA process is down.

Figure 42: Trap Details When NMA is Down

Request ID

737117913

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:10m:01.17s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	NMA stopped
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.2
mib-2.88.2.1.5.0	Integer	103
extNames.2	String	NMA
extOutput.2	String	

Close

Show Raw

<< prev

next >>

Request ID

737117913

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:10m:01.17s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	NMA stopped
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.2
1.3.6.1.2.1.88.2.1.5.0	Integer	103
1.3.6.1.4.1.2021.8.1.2.2	String	NMA
1.3.6.1.4.1.2021.8.1.101.2	String	

Close

Show Raw

<< prev

next >>

Table 87: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Webproxy

When the WebProxy process is up, the trap shown in Figure 43 on page 581 is generated:

Figure 43: WebProxy Is Up

<input type="checkbox"/>	390	space-000c29d796f5	1	3/27/14 12:12:55 [<] [>]	Process WebProxy started.
--------------------------	-----	--------------------	---	--------------------------	---------------------------

Figure 44 on page 581 shows the OID details for the trap generated when the WebProxy process is up.

Figure 44: Trap Details When WebProxy Is Up

Trap Details			Trap Details		
Request ID 1861139988			Request ID 1861139988		
Community public			Community public		
Error Index 0			Error Index 0		
Error Status 0			Error Status 0		
Ip Address 10.205.56.39			Ip Address 10.205.56.39		
Trap Type SNMPv2c			Trap Type SNMPv2c		
Variable Bindings			Variable Bindings		
OID	Type	Value	OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h 00m 05.49s	1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h 00m 05.49s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	webproxy started	1.3.6.1.2.1.88.2.1.1.0	String	webproxy started
mib-2.88.2.1.2.0	String		1.3.6.1.2.1.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String		1.3.6.1.2.1.88.2.1.3.0	String	
mib-2.88.2.1.4.0	String		1.3.6.1.2.1.88.2.1.4.0	String	
mib-2.88.2.1.5.0	Integer	102	1.3.6.1.2.1.88.2.1.5.0	Integer	102
extNames.1	String	Webproxy	1.3.6.1.4.1.2021.8.1.2.1	String	Webproxy
extOutput.1	String		1.3.6.1.4.1.2021.8.1.101.1	String	
Close Show Raw << prev next >>			Close Show Raw << prev next >>		

When the WebProxy process is down, the trap shown in Figure 45 on page 581 is generated:

Figure 45: WebProxy Is Down

<input type="checkbox"/>	386	space-000c29d796f5	1	3/27/14 12:12:24 [<] [>]	Process WebProxy stopped.
--------------------------	-----	--------------------	---	--------------------------	---------------------------

Figure 46 on page 581 shows the OID details for the trap generated when the WebProxy is down.

Figure 46: Trap Details When WebProxy Is Down

Trap Details			Trap Details		
Request ID 737109873			Request ID 737109873		
Community public			Community public		
Error Index 0			Error Index 0		
Error Status 0			Error Status 0		
Ip Address 10.205.56.39			Ip Address 10.205.56.39		
Trap Type SNMPv2c			Trap Type SNMPv2c		
Variable Bindings			Variable Bindings		
OID	Type	Value	OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h 01m 15.70s	1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h 01m 15.70s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	webproxy stopped	1.3.6.1.2.1.88.2.1.1.0	String	webproxy stopped
mib-2.88.2.1.2.0	String		1.3.6.1.2.1.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String		1.3.6.1.2.1.88.2.1.3.0	String	
mib-2.88.2.1.4.0	String		1.3.6.1.2.1.88.2.1.4.0	String	
mib-2.88.2.1.5.0	Integer	101	1.3.6.1.2.1.88.2.1.5.0	Integer	101
extNames.1	String	Webproxy	1.3.6.1.4.1.2021.8.1.2.1	String	Webproxy
extOutput.1	String		1.3.6.1.4.1.2021.8.1.101.1	String	
Close Show Raw << prev next >>			Close Show Raw << prev next >>		

Table 87: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: JBoss

When the JBoss process is up, the trap shown in Figure 47 on page 582 is generated:

Figure 47: JBoss Is Up

	394	space-000c29d796f5	1	3/27/14 12:14:46 [<] [>]	Process Jboss started.
---	-----	--------------------	---	--------------------------	------------------------

Figure 48 on page 582 shows the OID details for the trap generated when the JBoss process is up.

Figure 48: Trap Details When JBoss Is Up

Trap Details			Trap Details		
Request ID 1861140020			Request ID 1861140020		
Community public			Community public		
Error Index 0			Error Index 0		
Error Status 0			Error Status 0		
Ip Address 10.205.56.39			Ip Address 10.205.56.39		
Trap Type SNMPv2c			Trap Type SNMPv2c		
Variable Bindings			Variable Bindings		
OID	Type	Value	OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:00m:06.29s	1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:00m:06.29s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	Jboss started	1.3.6.1.2.1.88.2.1.1.0	String	Jboss started
mib-2.88.2.1.2.0	String		1.3.6.1.2.1.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String		1.3.6.1.2.1.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.3	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.3
mib-2.88.2.1.5.0	Integer	105	1.3.6.1.2.1.88.2.1.5.0	Integer	105
extNames.3	String	Jboss	1.3.6.1.4.1.2021.8.1.2.3	String	Jboss
extOutput.3	String		1.3.6.1.4.1.2021.8.1.101.3	String	
Close Show Raw << prev next >>			Close Show Raw << prev next >>		

When the JBoss process is down, the trap shown in Figure 49 on page 582 is generated:

Figure 49: JBoss Is Down


	391	space-000c29d796f5	1	3/27/14 12:13:01 [<] [>]	Process Jboss stopped.
---	-----	--------------------	---	--------------------------	------------------------

Figure 50 on page 582 shows the OID details for the trap generated when JBoss is down.

Figure 50: Trap Details When JBoss Is Down

Trap Details			Trap Details		
Request ID 737110115			Request ID 737110115		
Community public			Community public		
Error Index 0			Error Index 0		
Error Status 0			Error Status 0		
Ip Address 10.205.56.39			Ip Address 10.205.56.39		
Trap Type SNMPv2c			Trap Type SNMPv2c		
Variable Bindings			Variable Bindings		
OID	Type	Value	OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:31.41s	1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:31.41s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	Jboss stopped	1.3.6.1.2.1.88.2.1.1.0	String	Jboss stopped
mib-2.88.2.1.2.0	String		1.3.6.1.2.1.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String		1.3.6.1.2.1.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.3	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.3
mib-2.88.2.1.5.0	Integer	105	1.3.6.1.2.1.88.2.1.5.0	Integer	105
extNames.3	String	Jboss	1.3.6.1.4.1.2021.8.1.2.3	String	Jboss
extOutput.3	String		1.3.6.1.4.1.2021.8.1.101.3	String	
Close Show Raw << prev next >>			Close Show Raw << prev next >>		

Table 87: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Mysql

When the Mysql process is up, the trap shown in Figure 51 on page 583 is generated:

Figure 51: Mysql Is Up

<input type="checkbox"/>	392	space-000c29d796f5	1	3/27/14 12:13:07 [<] [>]	Process Mysql started.
--------------------------	-----	--------------------	---	--------------------------	------------------------

Figure 52 on page 583 shows the OID details for the trap generated when the Mysql process is up.

Figure 52: Trap Details When Mysql Is Up

Request ID

1861140036

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:00m:06.67s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mb-2.88.2.1.1.0	String	Mysql started
mb-2.88.2.1.2.0	String	
mb-2.88.2.1.3.0	String	
mb-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.4
mb-2.88.2.1.5.0	Integer	108
extNames.4	String	Mysql
extOutput.4	String	

Close

Show Raw

<< prev

next >>

Request ID

1861140036

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:00m:06.67s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Mysql started
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.4
1.3.6.1.2.1.88.2.1.5.0	Integer	108
1.3.6.1.4.1.2021.8.1.2.4	String	Mysql
1.3.6.1.4.1.2021.8.1.101.4	String	

Close

Show Raw

<< prev

next >>

When the Mysql process is down, the trap shown in Figure 53 on page 583 is generated:

Figure 53: Mysql Is Down

<input type="checkbox"/>	398	space-000c29d796f5	1	3/27/14 12:21:44 [<] [>]	Process Mysql stopped.
--------------------------	-----	--------------------	---	--------------------------	------------------------

Figure 54 on page 583 shows the OID details for the trap generated when the Mysql process is down.

Figure 54: Trap Details When Mysql Is Down

Request ID

737121741

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:14m:12.20s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mb-2.88.2.1.1.0	String	Mysql stopped
mb-2.88.2.1.2.0	String	
mb-2.88.2.1.3.0	String	
mb-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.4
mb-2.88.2.1.5.0	Integer	107
extNames.4	String	Mysql
extOutput.4	String	

Close

Show Raw

<< prev

next >>

Request ID

737121741

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:14m:12.20s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Mysql stopped
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.4
1.3.6.1.2.1.88.2.1.5.0	Integer	107
1.3.6.1.4.1.2021.8.1.2.4	String	Mysql
1.3.6.1.4.1.2021.8.1.101.4	String	

Close

Show Raw

<< prev

next >>

Table 87: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Postgresql

When the Postgresql process is up, the trap shown in [Figure 55 on page 584](#) is generated:

Figure 55: Postgresql Is Up

<input type="checkbox"/>	393	space-000c29d796f5	1	3/27/14 12:13:48 [<] [>]	Process Postgresql started.
--------------------------	-----	--------------------	---	--------------------------	-----------------------------

Figure 56 on [page 584](#) shows the OID details for the trap generated when the Postgresql process is up.

Figure 56: Trap Details When Postgresql Is Up

Trap Details

Request ID1861140052

Communitypublic

Error Index0

Error Status0

Ip Address10.205.56.39

Trap TypeSNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:00m:07.02s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mb-2.88.2.1.1.0	String	Postgresql started
mb-2.88.2.1.2.0	String	
mb-2.88.2.1.3.0	String	
mb-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.5
mb-2.88.2.1.5.0	Integer	110
extNames.5	String	Postgresql
extOutput.5	String	

Close

Show Raw

<< prev

next >>

Trap Details

Request ID1861140052

Communitypublic

Error Index0

Error Status0

Ip Address10.205.56.39

Trap TypeSNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:00m:07.02s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Postgresql started
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.5
1.3.6.1.2.1.88.2.1.5.0	Integer	110
1.3.6.1.4.1.2021.8.1.2.5	String	Postgresql
1.3.6.1.4.1.2021.8.1.101.5	String	

Close

Show Raw

<< prev

next >>

When the Postgresql process is down, the trap shown in [Figure 57 on page 584](#) is generated:

Figure 57: Postgresql Is Down

<input type="checkbox"/>	389	space-000c29d796f5	1	3/27/14 12:12:53 [<] [>]	Process Postgresql stopped.
--------------------------	-----	--------------------	---	--------------------------	-----------------------------

Figure 58 on [page 584](#) shows the OID details for the trap generated when the Postgresql process is up.

Figure 58: Trap Details When Postgresql Is Down

Trap Details

Request ID737120205

Communitypublic

Ip Address10.205.56.39

Error Index0

Error Status0

Trap TypeSNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:12m:32.66s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mb-2.88.2.1.1.0	String	Postgresql stopped
mb-2.88.2.1.2.0	String	
mb-2.88.2.1.3.0	String	
mb-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.5
mb-2.88.2.1.5.0	Integer	109
extNames.5	String	Postgresql
extOutput.5	String	

Close

Show Raw

<< prev

next >>

Trap Details

Request ID737120205

Communitypublic

Ip Address10.205.56.39

Error Index0

Error Status0

Trap TypeSNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:12m:32.66s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Postgresql stopped
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.8.1.100.5
1.3.6.1.2.1.88.2.1.5.0	Integer	109
1.3.6.1.4.1.2021.8.1.2.5	String	Postgresql
1.3.6.1.4.1.2021.8.1.101.5	String	

Close

Show Raw

<< prev

next >>

Table 87: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Free swap memory

When the free swap memory is greater than the upper threshold limit, the trap shown in Figure 59 on page 585 is generated:

Figure 59: Swap Memory Usage Is Normal

<input type="checkbox"/>	405	space-000c29d796f5	2	3/27/14 12:28:43 [<] [>]	Swap memory usage is normal.
--------------------------	-----	--------------------	---	--------------------------	------------------------------

Figure 60 on page 585 shows the OID details for the trap generated when swap memory usage is normal.

Figure 60: Trap Details When Swap Memory Is Normal

Request ID

1861140788

Community

public

Ip Address

10.205.56.39

Error Index

0

Error Status

0

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.11s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	Swap memory clear
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.4.100.0
mib-2.88.2.1.5.0	Integer	0
memErrorName.0	String	swap
memSwapErrorMsg.0	String	

Close

Show Raw

<< prev

next >>

Request ID

1861140788

Community

public

Ip Address

10.205.56.39

Error Index

0

Error Status

0

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.11s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Swap memory clear
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.4.100.0
1.3.6.1.2.1.88.2.1.5.0	Integer	0
1.3.6.1.4.1.2021.4.2.0	String	swap
1.3.6.1.4.1.2021.4.101.0	String	

Close

Show Raw

<< prev

next >>

When the free swap memory is less than the upper threshold limit, the trap shown in Figure 61 on page 585 is generated:

Figure 61: Swap Memory Usage Threshold Exceeds Upper Limit

<input type="checkbox"/>	410	space-000c29d796f5	1	3/27/14 12:30:56 [<] [>]	Swap memory usage threshold upper limit exceeded . Running out of swap space (8191420).
--------------------------	-----	--------------------	---	--------------------------	---

Figure 62 on page 585 shows the OID details for the trap generated when swap memory usage is exceeds upper limit.

Figure 62: Trap Details When Swap Memory Usage Exceeds Upper Limit

Request ID

1314711189

Community

public

Ip Address

10.205.56.39

Error Index

0

Error Status

0

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.10s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	Swap memory trigger
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.4.100.0
mib-2.88.2.1.5.0	Integer	1
memErrorName.0	String	swap
memSwapErrorMsg.0	String	Running out of swap space (200630368)

Close

Show Raw

<< prev

next >>

Request ID

1314711189

Community

public

Ip Address

10.205.56.39

Error Index

0

Error Status

0

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.10s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	Swap memory trigger
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.4.100.0
1.3.6.1.2.1.88.2.1.5.0	Integer	1
1.3.6.1.4.1.2021.4.2.0	String	swap
1.3.6.1.4.1.2021.4.101.0	String	Running out of swap space (200630368)

Close

Show Raw

<< prev

next >>

Table 88 on page 586 shows the configuration parameters for monitoring Junos Space Network Management Platform hardware.

Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware

Monitoring Linux Hardware
<p>NOTE: LM-SENSORS-MIB is not supported by the Junos Space Virtual Appliance, but only by the Junos Space Appliance. Therefore the threshold settings of CPU Max Temp (mC), CPU Min Fan (RPM) and CPU Min Voltage (mV) will not trigger any traps in the virtual appliance.</p>

Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware (*continued*)

Monitoring Linux Hardware

Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware (*continued*)


Monitoring Linux Hardware

Parameter: CPU min FAN (rpm)

Default Threshold Value: 1500

When the CPU fan speed is greater than the configured threshold (minimum fan speed), the trap shown in [Figure 63 on page 588](#) is generated:

Figure 63: CPU Fan Speed Normal

	41	space-0256102011000007	1	3/27/14 12:44:58 [<] [>]	CPU fan is normal.
---	----	------------------------	---	--------------------------	--------------------

[Figure 64 on page 588](#) shows the OID details for the trap generated when CPU fan speed is normal.

Figure 64: Trap Details When CPU Fan Speed Is Normal

Trap Details

Request ID: 1861140860
Community: public
Ip Address: 10.205.56.39
Error Index: 0
Error Status: 0
Trap Type: SNMPv2c

Variable Bindings:

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.13s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	CPU fan clear
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.13.16.3.1.3.2
mib-2.88.2.1.5.0	Gauge	5818

Close Show Row << prev next >>

Trap Details

Request ID: 1861140860
Community: public
Ip Address: 10.205.56.39
Error Index: 0
Error Status: 0
Trap Type: SNMPv2c


Variable Bindings:

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.13s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	CPU fan clear
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.13.16.3.1.3.2
1.3.6.1.2.1.88.2.1.5.0	Gauge	5818

Close Show Row << prev next >>

When the CPU fan speed is less than the configured threshold (minimum fan speed), the trap shown in [Figure 65 on page 588](#) is generated:

Figure 65: CPU Fan Speed Is Below the Configured Threshold

	280	space-0256042012000014	1	3/28/14 12:33:16 [<] [>]	CPU fan too slow (rpm):5625.
---	-----	------------------------	---	--------------------------	------------------------------

[Figure 66 on page 588](#) shows the OID details for the trap generated when CPU fan speed lower than the configured threshold.

Figure 66: Trap Details When CPU Fan Speed Is Below the Configured Threshold

Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware (*continued*)

Monitoring Linux Hardware

Trap Details

Request ID

709619518

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h 01m 00.12s
ringTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	CPU fan trigger
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.13.16.3.1.3.2
mib-2.88.2.1.5.0	Gauge	5625

Close

Show Raw

<< prev

next >>

Trap Details

Request ID

709619518

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h 01m 00.12s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	CPU fan trigger
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.13.16.3.1.3.2
1.3.6.1.2.1.88.2.1.5.0	Gauge	5625

Close

Show Raw

<< prev

next >>

Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware (*continued*)

Monitoring Linux Hardware

Parameter: CPU min Voltage (mV)

When the CPU voltage is greater than the configured value, the trap shown in Figure 67 on page 590 is generated:

Figure 67: CPU Voltage Normal

42	space-0256102011000007	1	3/27/14 12:44:58 [<] [>]	CPU voltage is normal.
----	------------------------	---	--------------------------	------------------------

Figure 68 on page 590 shows the OID details for the trap generated when CPU voltage is normal.

Figure 68: Trap Details When CPU Voltage Is Normal

The figure shows two identical screenshots of the 'Trap Details' window. The window displays the following information:

- Request ID:** 1314711267
- Community:** public
- Error Index:** 0
- Error Status:** 0
- Ip Address:** 10.205.56.39
- Trap Type:** SNMPv2c
- Variable Bindings:**

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.11s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mb-2.88.2.1.1.0	String	CPU voltage clear
mb-2.88.2.1.2.0	String	
mb-2.88.2.1.3.0	String	
mb-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.13.16.4.1.3.2
mb-2.88.2.1.5.0	Gauge	3328

Buttons at the bottom include 'Close', 'Show Raw', '<< prev', and 'next >>'.

Default Threshold Value: 1000

When the CPU voltage is lower than the configured value, the trap shown in Figure 69 on page 590 is generated:

Figure 69: CPU Voltage Is Lower Than Configured Threshold

60	space-0256102011000007	1	3/27/14 12:58:20 [<] [>]	CPU voltage too low (mV):3328.
----	------------------------	---	--------------------------	--------------------------------

Figure 70 on page 590 shows the OID details for the trap generated when CPU voltage is lower than the configured threshold.

Figure 70: Trap Details When CPU Voltage Is Lower Than Configured Threshold

The figure shows two identical screenshots of the 'Trap Details' window. The window displays the following information:

- Request ID:** 1861140863
- Community:** public
- Error Index:** 0
- Error Status:** 0
- Ip Address:** 10.205.56.39
- Trap Type:** SNMPv2c
- Variable Bindings:**

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h:01m:00.13s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mb-2.88.2.1.1.0	String	CPU voltage trigger
mb-2.88.2.1.2.0	String	
mb-2.88.2.1.3.0	String	
mb-2.88.2.1.4.0	OID	1.3.6.1.4.1.2021.13.16.4.1.3.2
mb-2.88.2.1.5.0	Gauge	3312

Buttons at the bottom include 'Close', 'Show Raw', '<< prev', and 'next >>'.

Table 88: SNMP Configuration Parameters: Monitoring Linux Hardware (*continued*)

Monitoring Linux Hardware

Parameter: CPU Temperature

When the CPU temperature is lower than the configured threshold, the trap shown in Figure 71 on page 591 is generated:

Figure 71: CPU Temperature Normal

<input type="checkbox"/>	260	space-0256042012000014	4	3/28/14 12:33:16 [<] [>]	CPU temperature is normal.
--------------------------	-----	------------------------	---	--------------------------	----------------------------

Figure 72 on page 591 shows the OID details for the trap generated when CPU temperature is normal.

Figure 72: Trap Details When CPU Temperature Is Normal

Trap Details

Request ID

737109630

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h 01m 00.12s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	CPU temperature clear
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	String	
mib-2.88.2.1.5.0	Gauge	1.3.6.1.4.1.2021.13.16.2.1.3.2 47500

Close

Show Raw

<< prev

next >>

Trap Details

Request ID

737109630

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h 01m 00.12s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	CPU temperature clear
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	String	
1.3.6.1.2.1.88.2.1.5.0	Gauge	1.3.6.1.4.1.2021.13.16.2.1.3.2 47500

Close

Show Raw

<< prev

next >>

When the CPU temperature exceeds the configured threshold, the trap shown in Figure 73 on page 591 is generated:

Figure 73: CPU Temperature Exceeds The Configured Threshold

<input type="checkbox"/>	40	space-0256102011000007	1	3/27/14 12:44:58 [<] [>]	CPU temperature too high(mC):51000.
--------------------------	----	------------------------	---	--------------------------	-------------------------------------

Figure 74 on page 591 shows the OID details for the trap generated when CPU temperature is higher than the configured threshold.

Figure 74: Trap Details When CPU Temperature Exceeds The Configured Threshold

Trap Details

Request ID

1861140855

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
sysUpTime.0	TimeTick	0 days 00h 01m 00.12s
snmpTrapOID.0	OID	1.3.6.1.2.1.88.2.0.1
mib-2.88.2.1.1.0	String	CPU temperature trigger
mib-2.88.2.1.2.0	String	
mib-2.88.2.1.3.0	String	
mib-2.88.2.1.4.0	String	
mib-2.88.2.1.5.0	Gauge	1.3.6.1.4.1.2021.13.16.2.1.3.2 47500

Close

Show Raw

<< prev

next >>

Trap Details

Request ID

1861140855

Community

public

Error Index

0

Error Status

0

Ip Address

10.205.56.39

Trap Type

SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h 01m 00.12s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1
1.3.6.1.2.1.88.2.1.1.0	String	CPU temperature trigger
1.3.6.1.2.1.88.2.1.2.0	String	
1.3.6.1.2.1.88.2.1.3.0	String	
1.3.6.1.2.1.88.2.1.4.0	String	
1.3.6.1.2.1.88.2.1.5.0	Gauge	1.3.6.1.4.1.2021.13.16.2.1.3.2 47500

Close

Show Raw

<< prev

next >>



.....

NOTE: LM-SENSORS-MIB is not supported by the Junos Space Virtual Appliance, but only by the Junos Space Appliance. Therefore the threshold settings of CPU Max Temp (mC), CPU Min Fan (RPM) and CPU Min Voltage (mV) will not trigger any traps in the virtual appliance.

.....



.....

NOTE: Junos Space supports Raid related traps on a Junos Space Physical appliance. The following is a sample trap:

.....

```
40948 Normal [+] [-] 2/4/13 09:54:14 [<] [>] space-node 10.205.56.38
[+] [-]
uei.opennms.org/generic/traps/EnterpriseDefault [+] [-] Edit
notifications for event
Received unformatted enterprise event (enterprise:.1.3.6.1.4.1.8072.4
generic:6 specific:1001). 1 args: .1.3.6.1.4.1.795.14.1.9000.1="One or
more logical devices contain a bad stripe: controller 1."
```

.....

**NOTE:**

For an external SNMP Manager, the “Junos Space MIB” should be compiled to receive the following events in formatted manner:

- Junos Space Node Down

Figure 75 on page 593 shows the OID details for the trap generated when Junos Space node is down.

Figure 75: Trap Details Junos Space Node Is Down

The figure shows two screenshots of the Junos Space Trap Details window. Both windows display the following information:

- Request ID: 191543944
- Community: JUNIPER
- Error Index: 0
- Error Status: 0
- Ip Address: 10.205.55.136
- Trap Type: SNMPv2c

The Variable Bindings table for both events is as follows:

OID	Type	Value
sysUpTime.0	TimeTick	0 days 09h 03m 43.90s
snmpTrapOID.0	OID	1.3.6.1.4.1.2536.1.3.1.1.1
jnxSpaceNodeIP	IpAddress	10.205.55.77

- Junos Space Node Up

Figure 76 on page 593 shows the OID details for the trap generated when Junos Space node is up.

Figure 76: Trap Details Junos Space Node Is Up

The figure shows two screenshots of the Junos Space Trap Details window. Both windows display the following information:

- Request ID: 2351095485
- Community: JUNIPER
- Error Index: 0
- Error Status: 0
- Ip Address: 10.205.55.136
- Trap Type: SNMPv2c

The Variable Bindings table for both events is as follows:

OID	Type	Value
sysUpTime.0	TimeTick	0 days 07h 12m 37.70s
snmpTrapOID.0	OID	1.3.6.1.4.1.2536.1.3.1.1.2
jnxSpaceNodeIP	IpAddress	10.205.55.77

- Delete Junos Space Node

Figure 77 on page 593 shows the OID details for the trap generated when Junos Space node is deleted.

Figure 77: Trap Details Junos Space Node Is Deleted

OID	Type	Value
sysUpTime.0	TimeTick	0 days 07h20m44.75s
snmpTrapOID.0	OID	461spacePlatformTraps
nmSpaceNodeIP	IpAddress	10.205.96.77
nmSpaceObjectState	String	Space node removed successful

Starting SNMP Monitoring on Fabric Nodes

To start SNMP monitoring on one or more fabric nodes:

1. Select **Network Management Platform > Administration > Fabric**.

The Fabric page appears.

2. Select the check box for each fabric node on which you want to start SNMP monitoring.
3. From the Actions menu, select **SNMP Start**.

The Confirm Start SNMP Agent dialog box is displayed.

4. Click **Yes**.

Junos Space begins SNMP monitoring on the selected fabric nodes.



NOTE: This process might take a while.

5. To view the status of SNMP monitoring on the selected fabric nodes, select **Network Monitoring > Node List**.

The Network Monitoring > Node List page appears.

6. Select the node on which you started the SNMP monitoring.

The VIP node is represented as **space-*<number>* (ID: 1)**. It is easier to identify the VIP node using the “ID: 1” text.

Figure 78 on page 595 shows a sample view of network monitoring details for the selected fabric node.

Figure 78: 6412-monitoring-nodes-netmon-node-list

The screenshot displays the 'Node List' page in the Junos Space Network Monitoring interface. The page is divided into several sections:

- SNM Attributes:**
 - Name: space-0256042012000017
 - Object ID: .1.3.6.1.4.1.8072.3.2.10
 - Location: unknown
 - Contact: root
 - Description: Linux space-0256042012000017 2.6.18-274.el5 #1 SMP Fri Jul 22 04:43:29 EDT 2011 x86_64
- Availability:**
 - Availability (last 24 hours): 94.751%
 - 10.205.56.40: Overall 92.126%, ICMP 100.000%
 - 10.205.57.40: Overall 100.000%, ICMP 100.000%
- Node Interfaces:**
 - IP Interfaces:

IP Address	IP Host Name	ifIndex	Managed
10.205.56.40	10.205.56.40		M
10.205.57.40	10.205.57.40	2	M
- General (Status: Active):**
 - View Node Link Detailed Info
 - Surveillance Category Memberships (Edit): Fabric, Medium, Monitor_SNM
- Notification:**
 - You: Outstanding: (Check)
 - You: Acknowledged: (Check)
- Recent Events:**
 - 74576: 10/3/12 15:25:30, Normal, SNMP data collection on interface 10.205.56.40 previously failed and has been restored.
 - 74321: 10/3/12 15:23:33, Normal, The SNMP outage on interface 10.205.56.40 has been cleared. Service is restored.
 - 73212: 10/3/12 15:13:19, Minor, SNMP outage identified on interface 10.205.56.40 with reason code: SNMP poll failed, addr=10.205.56.40 oid=.1.3.6.1.2.1.1.2.0.
 - 73209: 10/3/12 15:13:17, Minor, SNMP data collection on interface 10.205.56.40 failed with Timeout retrieving SnmpCollectors for 10.205.56.40 for /10.205.56.40: SnmpCollectors for 10.205.56.40: snmpTimeoutError /10.205.56.40/
 - 73291: 10/3/12 14:52:11, Warning, jnxNetworkMonitoringStart trap received
- Recent Outages:**

Interface	Service	Lost	Regained	Outage ID
-----------	---------	------	----------	-----------

Under Notification / Recent Events on the right of the Node List page, you see the results of the SNMP monitoring operation.

Stopping SNMP Monitoring on Fabric Nodes

To stop SNMP monitoring on one or more fabric nodes:

1. Select **Network Management Platform > Administration > Fabric**.

The Fabric page appears.

2. Select the check box for each fabric node on which you want to stop SNMP monitoring.
3. From the Actions menu, select **SNMP Stop**.

The Confirm Stop SNMP Agent dialog box is displayed.

4. Click **Yes**.

Junos Space stops SNMP monitoring on the selected fabric nodes.

Restarting SNMP Monitoring on Fabric Nodes

To restart SNMP monitoring on one or more fabric nodes:

1. Select **Network Management Platform > Administration > Fabric**.

The Fabric page appears.

2. Select the check box for each fabric node on which you want to restart SNMP monitoring.
3. From the Actions menu, select **SNMP Restart**.

The Confirm Restart SNMP Agent dialog box is displayed.

4. Click **Yes**.

Junos Space restarts SNMP monitoring on the selected fabric nodes.

Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node

To add a third-party SNMP V1 or V2c manager on a fabric node:

1. Select **Platform > Administration > Fabric > SNMP Manager**.

The SNMP Manager page appears.

2. Click the **Add SNMP Manager** icon.

The Add 3rd Party SNMP Manager dialog box is displayed.

3. In the **Manager IP** field, enter the SNMP manager IP address.



NOTE: The IPv4 address that you use must be a valid address. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses.

4. In the **Version** field, select the SNMP version (V1 or V2c) .

5. In the **Community** field, enter the community string.

Any alphanumeric string is acceptable, including spaces and symbols, from 1 to 2,147,483,647 characters.

6. Click **OK**.

The newly added SNMP v1 or v2c Manager is displayed on the SNMP Manager page.

Adding a Third-Party SNMP V3 Manager on a Fabric Node

To add a third-party SNMP third-party3 manager on a fabric node:

1. Select **Platform > Administration > Fabric > SNMP Manager**.

The SNMP Manager page appears.

2. Click the **Add** icon.

The Add 3rd Party SNMP Manager dialog box displays.

3. In the **Manager IP** field, enter the SNMP manager IP address.



NOTE: The IPv4 address that you use must be a valid address. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses.

4. In the **Version** field, select V3.

5. In the **User Name** field, type 1 through 2,147,483,647 alphanumeric characters, including spaces and symbols to identify the user.
6. In the **Authentication Type** field, enter the authentication type (**MD5** or **SHA**).
7. In the **Authentication Password** field, enter the authentication password. You can type 1 through 2,147,483,647 alphanumeric characters, including spaces and symbols.
8. In the **Confirm Authentication password**, enter the authentication password again to confirm the password.

Any alphanumeric string is acceptable, including spaces and symbols, from 1 to 2,147,483,647 characters.

9. From the **Security Level** list, select the security level:

- **noAuthNoPriv**
- **authNoPriv**
- **authPriv**

10. In the **Privacy Type** field, enter the privacy type (**AES** or **DES**).

11. In the **Privacy Password** field, enter the privacy password.

Any alphanumeric string is acceptable, including spaces and symbols, from 1 to 2,147,483,647 characters.

12. In the **Confirm Privacy password** field, enter the privacy password again to confirm the password.

You can type 1 through 2,147,483,647 alphanumeric characters, including spaces and symbols.

13. Click **OK**.

The newly added SNMP Manager entry is displayed on the SNMP Manager page.

Deleting a Third-Party SNMP Manager from a Fabric Node

To delete a third-party SNMP manager configuration from a fabric node:

1. Select **Platform > Administration > Fabric > SNMP Manager**.

The SNMP Manager page appears.

2. Select the SNMP manager configuration that you want to remove.

3. Click the **Delete SNMP Manager** icon.

4. To confirm the deletion of the SNMP manager, click **Yes**.

The deleted SNMP manager is removed from the SNMP Manager page.

Related Documentation

- [Overall System Condition and Fabric Load History Overview on page 568](#)
- [Fabric Management Overview on page 551](#)
- [Junos Space User Interface Overview on page 9](#)

- [Viewing Nodes in the Fabric on page 557](#)

Creating a System Snapshot

You can use the System Snapshot feature to create a snapshot of the system state and rollback the system to a predefined state. The snapshot includes all persistent data on the hard disk including data in the database, system and application configuration files, and application and Linux executables. The System Snapshot is a fabric-wide operation that maintains consistency across all nodes in the fabric.

Typically, you would use the System Snapshot feature for rolling back the system when it is in an unrecoverable error-state due to corruption of system files, interruption of critical processes, and so on. You can also roll back the system to an older release if the system exhibits undesirable behaviors after a software version upgrade.



TIP: We recommend using System Snapshot before performing significant actions (Add/Delete Node, Application Installation) and such actions that have the potential to precipitate the system into an undesirable state. You can delete the snapshot after you have ascertained that these actions were performed successfully.

System Snapshot is currently supported on a Junos Space fabric that consists of only Junos Space VM or only Junos Space Appliance. This feature is not supported on a hybrid fabric consisting of both Junos Space VM and Junos Space Appliance.

System Snapshot does not impact the performance of a Junos Space VM. However, if you are using a Junos Space Appliance, performance may be impacted by the number of write operations performed to the snapshot's logical volume.

The maximum size that a snapshot can occupy for a new 11.3 Space Platform is 300GB. The maximum size that a snapshot can occupy for a Junos Space Network Management Platform migrated from releases prior to 11.3 is 43GB. On the Real Appliance, the snapshot will become invalid if it has been kept for a long time, because the snapshot volume disk space usage increases as write operations continue. Once the usage reaches the maximum size of snapshot volume, the snapshot will be disabled. Therefore, ensure that you clear enough hard disk space to accommodate the snapshot.

If you are upgrading Junos Space Network Management Platform from releases prior to 11.3, perform the following steps before using the System Snapshot feature:

1. Connect the recovery USB/CD to Junos Space Appliance, and reboot to set USB/CD as the first boot option.
2. Restart the box, and choose the **rescue-serial** mode while booting.
3. Follow the on-screen steps and choose **Skip** when asked whether you want to find an existing Space installation and mount to mnt/sysimage.
4. Once you are in the recovery shell, execute the following sequence of commands:

- a. `lvm vgchange -ay jmpvgnocf`
- b. `e2fsck -f /dev/jmpvgnocf/lvroot`
- c. `resize2fs -f /dev/jmpvgnocf/lvroot 900G`
- d. `lvm lvreduce -L1024G /dev/jmpvgnocf/lvroot`
- e. `resize2fs -f /dev/jmpvgnocf/lvroot`

After executing these commands, start creating the snapshot. The steps used to create a system snapshot for a Junos Space VM and a Junos Space Appliance are almost identical, but there are two additional preliminary steps for the Junos Space VM:

If you are working with a Junos Space VM:

- a. Select **Administration > Fabric** and set the ESX configuration for every node in the fabric.
- b. Install the VI Toolkit for Perl provided by VMware.

To create a system snapshot:

1. Select **Administration > Fabric** and select the **System Snapshot** icon.

The System Snapshot dialog box appears. You can see a system snapshot if you have taken a snapshot earlier. If you are taking the snapshot for the first time, you will not see any snapshots in this dialog box.



NOTE: If you are creating a system snapshot when a snapshot already exists, the new snapshot will overwrite the older snapshot. Currently Junos Space Network Management Platform can store only one System Snapshot.

2. Click **Take Snapshot**.

The System Snapshot Confirmation dialog box appears.

3. Enter the name of the snapshot in the **Snapshot Name** box.
4. Enter the comments in the **Comment** box.
5. Click **Confirm**.

A new job is created and the job ID appears in the System Snapshot Job Information dialog box.

6. Click the job ID to view more information about the job created. This action directs you to the Job Management work space.

The time taken to complete the snapshot job for a VM is dependent on the number of nodes in the fabric, the disk size of the VM, the memory size of the VM, and the performance of the ESX server. The time taken to complete the snapshot job for a Junos Space Appliance is dependent on the disk space used on the appliance.



NOTE: You may not be able to create a snapshot of the system state if any of the following conditions are true:

- Insufficient disk space on ESX servers.
- Mis-configuration on one of the ESX servers.
- One of the nodes is down.
- Hybrid fabric consisting of both Junos Space VM and Junos Space Appliance.
- The name specified for the current snapshot is the same as that of the stored snapshot.

Related Documentation

- [Deleting a System Snapshot on page 600](#)
- [Restoring the System to a Snapshot on page 600](#)

Deleting a System Snapshot

To delete a System Snapshot:

1. Select **Administration > Fabric >** and select the **System Snapshot** icon.
2. Click **Delete**.

The System Snapshot Deletion dialog box appears. A new job is created and the job ID appears in the System Snapshot Job Information dialog box.

3. Click the job ID to view more information about the job created. This action directs you to the Job Management work space.



NOTE: You may not be able to delete a snapshot of the system state if any of the following conditions are true:

- Mis-configuration on one of the ESX servers.
- Hybrid fabric consisting of both Junos Space VM and Junos Space Appliance.
- Snapshot does not exist.

Related Documentation

- [Creating a System Snapshot on page 598](#)
- [Restoring the System to a Snapshot on page 600](#)

Restoring the System to a Snapshot

The process to restore a system to a snapshot differs depending on whether you are using a Junos Space VM or a Junos Space Appliance.

To restore a system snapshot when using a VM:

1. Select **Administration** > **Fabric** and select the **System Snapshot** icon.
2. Click **Restore**.
3. Click **OK**.
4. Login to the ESX servers and power on the VM after few minutes.



NOTE: If the Space GUI is not accessible on a VM, you can restore the fabric by shutting down every node in the fabric and logging into ESX servers where the VM is located.

To restore a System Snapshot when using a Junos Space Appliance:

1. Select **Administration** > **Fabric** and select the **System Snapshot** icon.
2. Click **Restore**.

The System Restore Instruction for Appliance dialog box appears.

3. Follow the instructions on this dialog box.
4. Click **OK**.



NOTE: You may not be able to restore the system to a snapshot if one of the following conditions are true:

- One of the nodes is down.
- New nodes were added after a snapshot was created. A warning message that prompts you to delete the new nodes before restoring is shown.
- Some nodes were deleted after a snapshot was created. A warning message that prompts you to restore the nodes before restoring is shown.

- Related Documentation**
- [Creating a System Snapshot on page 598](#)
 - [Deleting a System Snapshot on page 600](#)

CHAPTER 62

Managing Databases

- [Backing Up and Restoring the Database on page 604](#)
- [Backing Up the Database on page 605](#)
- [Restoring a Database in the User Interface on page 610](#)
- [Viewing Database Backup Files on page 613](#)
- [Deleting Database Backup Files on page 614](#)
- [Viewing Job Recurrence on page 615](#)

Backing Up and Restoring the Database

As system administrator, you can perform Junos Space Network Management Platform database backup, restore, and delete operations. From Junos Space Network Management Platform Release 13.1 onward, Junos Space Network Management Platform enables you to back up the complete system data, which includes the MySQL database as well as the network monitoring database (containing the PostgreSQL data, configuration files, and performance data files). Because of this feature, if a system crashes, you can add a new system (RMA) and restore the configuration that was existing in the crashed system from the backup file.

To perform database backup or restore operations, you must be assigned the system administrator role. Only a system administrator can initiate a backup from the Administration > Backup and Restore workspace.

When you initiate a backup, all databases are backed up by default. Because the network monitoring database could be fairly large in size, you can select whether or not to back up this database from the Junos Space GUI. If sufficient disk space is unavailable, Junos Space Network Management Platform throws an error. Duration of the backup job might vary depending on the database size.

Junos Space Network Management Platform allows you to perform backup and restore operations even when the network monitoring service is turned off.



NOTE: For disaster recovery, different, additional database backup and restore provisions must be made. See [“Understanding Disaster Recovery” on page 734](#).

Restore the Junos Space Network Management Platform database if any of the following conditions occur:

- Junos Space Network Management Platform data is corrupted, and you need to replace it with uncorrupted data.
- The Junos Space Network Management Platform software became corrupted, and you reinstalled the Junos Space Network Management Platform software.
- You can restore a Junos Space database from a backup that is taken in the same release version only. For example, you can restore a Junos Space Release xx database only from a backup that is taken in Junos Space Release xx, where xx represents the version number.

Backing up a Database

By default, Junos Space Network Management Platform automatically backs up the database once a week. However, the administrator can schedule a backup to run at anytime and perform either local or remote backups. All jobs that completed prior to the time the backup operation starts are captured in the database backup file.

During a backup, Junos Space Network Management Platform archives data files and the logical logs that record database transactions, such as the users, nodes, devices, and added or deleted services in Junos Space Network Management Platform.

The administrator can perform a local or remote database backup. When the administrator performs a local backup, Junos Space Network Management Platform backs up all database data and log files to a local default directory `/var/cache/jboss/backup`. You cannot specify a different database backup file location for a local backup. No such restriction exists when backing up to a remote location.

For a remote backup, use only a Linux-based server. You must specify a remote host that is configured to run the Linux Secure Copy (SCP) command. You must also specify a valid user ID and password for the remote host. To ensure that you are using a valid directory, check the destination directory before you initiate a database backup to the remote system.

For instructions on how to back up the Junos Space Network Management Platform database, see [“Backing Up the Junos Space Network Management Platform Database” on page 605](#).

Restoring a Database

When the system administrator performs a restore database operation, data from a previous database backup is used to restore the Junos Space Network Management Platform database to a previous state. The administrator can restore the database from the Junos Space user interface (Administration > Backup and Restore workspace) (see [“Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface” on page 610](#)).

The database restoration operation is done while Junos Space Network Management Platform is in maintenance mode. The system is therefore down on all nodes in the fabric and only the web proxy is running. During this time, all Junos Space users, except the maintenance mode administrator, are locked out of the Junos Space system.



NOTE: After the Junos Space Network Management Platform database is restored, a manual re-index of the Security Design database is required. For more information on this, see the Security Design documentation.

Related Documentation

- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 610](#)
- [Backing Up the Junos Space Network Management Platform Database on page 605](#)
- [Maintenance Mode Overview on page 548](#)

Backing Up the Database

The system administrator can make a backup copy of the Junos Space Network Management Platform database and, at a later time, use the backup file to restore the

Junos Space Network Management Platform database to a previous state. The database backup file contains configuration data for managed nodes, managed devices, deployed services, scheduled jobs, Junos Space Network Management Platform users, network monitoring, and so forth.

The administrator can perform local and remote backup and restore operations. You perform a local backup to copy the backup file to the default directory `/var/cache/jboss/backup`. You perform a remote backup to copy the backup file to remote network hosts or media.

This topic includes the following tasks:

- [Backing Up the Database to a Local Directory on page 606](#)
- [Backing Up the Database to a Remote Host on page 608](#)

Backing Up the Database to a Local Directory

To back up the Junos Space Network Management Platform database to a local directory:

1. Select **Administration** > **Backup and Restore** and select the Database Backup icon.

The Backup page appears. The default behavior is a backup occurring once weekly (see the **Repeat** section on the Backup page).

2. In the **Mode** field, select **local** to back up the Junos Space Network Management Platform database to the default directory `/var/cache/jboss/backup`.



NOTE: When you select the local mode option, the Username, Password, Confirm password, Machine IP, and Directory text boxes on the Backup page are disabled.

3. Retain the selection of **Network Monitoring** under the **Content Options** section for Junos Space Network Management Platform to back up network monitoring data, in addition to the default MySQL data.

Clear the **Network Monitoring** check box to back up only MySQL data.

If you choose to back up network monitoring data, then the following information is backed up:

- PostgreSQL network monitoring database
- Configuration files that reside under the “**etc**” directory and its subdirectories
- Graphs data that reside under the “**rrd**” directory and its subdirectories



NOTE: By default, MySQL data is backed up. In the GUI, the **MySQL** check box is selected and disabled.

4. (Optional) In the **Comment** box, add a comment to describe or otherwise identify the backup operation.

5. (Optional) Schedule the Junos Space Network Management Platform database backup operation to occur at a later time.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the database backup.
 - Clear the **Schedule at a later time** check box (the default) to initiate the database backup as soon as you click **Backup**.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

6. (Optional) Schedule database backup recurrence by selecting **Repeat**.
 - a. Specify the database backup recurrence by setting the interval and the increment. The default recurrence interval is 1 hour.

Table 89: Backup Schedule Units and Increments

Unit of Time	Increment
Minutes	1-59
Hours	12:00 AM - 11:45 PM
Days	1-6
Weeks	1-4
Weekdays	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
Months	1-12, plus date of recurrence expressed as a date, and as one the first, second, third, fourth or last Monday-Sunday of the month.
Years	1-50, plus date of recurrence expressed as a date, and as one the first, second, third, fourth or last Monday-Sunday of the month.

- b. Specify when the recurrence should end.

Indicate a date and time. You can use the date calendar and the time list. If you do not specify an end, the database backup will recur endlessly until you cancel the job manually.

7. Click **Backup**.

The database is backed up. The **Backup Job Information** dialog box appears.
8. (Optional) Click the Job ID in the Backup Job Information dialog box to view the database backup job details in the View Job Details dialog box.
9. Click **OK**.

The Junos Space Network Management Platform database backup appears on the Backup and Restore inventory page. See [“Viewing Scheduled Jobs” on page 466](#).

All the backup files are compressed into a single .tgz file with the naming convention of “backup_ + timestamp + .tgz”. The backup file contains either MySQL and network monitoring data, or just MySQL data depending on whether you have chosen to back up both or just one of the databases.

Backing Up the Database to a Remote Host

The protocol used to transfer the database backup to a remote host is SCP, Secure Copy Protocol.

To back up the Junos Space Network Management Platform database to a remote host:

1. Select **Administration > Backup and Restore** and select the Database Backup icon.

The Backup page appears.

2. In the **Mode** field, select **remote**.
3. Enter a username to access the remote host server.
4. Enter the corresponding password.
5. Reenter the password.
6. Enter the remote host server IP address.
7. Enter a directory path on the remote host server for the database backup file.



NOTE: The directory path must already exist on the remote host server.

8. Retain the selection of **Network Monitoring** under the **Content Options** section for Junos Space Network Management Platform to back up network monitoring data, in addition to the default MySQL data.

Clear the **Network Monitoring** check box to back up only MySQL data.

If you choose to back up network monitoring data, then the following information is backed up:

- PostgreSQL network monitoring database
- Configuration files that reside under the “etc” directory and its subdirectories
- Graphs data that reside under the “rrd” directory and its subdirectories



NOTE: By default, MySQL data is backed up. In the GUI, the MySQL check box is selected and disabled.

9. (Optional) Add a comment to describe or otherwise identify the backup operation.

10. (Optional) Schedule the Junos Space Network Management Platform database backup operation to occur at a later time.

- Select the **Schedule at a later time** check box to specify a later start date and time for the database backup.
- Clear the **Schedule at a later time** check box (the default) to initiate the database backup as soon as you click **Backup**.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

11. Optional: Schedule database backup recurrence by selecting **Repeat**.

- a. Specify the database backup recurrence by setting the interval and the increment. See [Table 89 on page 607](#).

When applicable, specify a time interval. The default recurrence interval is 1 hour.

- b. Specify when the recurrence should end.

Indicate a date and time. You can use the date calendar and the time list. If you do not specify an end, the database backup will recur endlessly until you cancel the job manually.

12. Click **Backup**. The database backup occurs.

The Backup Job Information dialog box appears.

13. (Optional) Click the Job ID in the Backup Job Information dialog box to view job details for the database backup. The View Job Details dialog box appears.

14. Click **OK** to close the View Job Details dialog box.

When the backup operation finishes, the Junos Space Network Management Platform database backup file appears in the Backup and Restore inventory page.

All the backup files are compressed into a single .tgz file with the naming convention of "backup_ + timestamp + .tgz". The backup file contains either MySQL and network monitoring data, or just MySQL data depending on whether you have chosen to back up both or just one of the databases.

Related Documentation

- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 610](#)
- [Viewing Database Backup Files on page 613](#)
- [Deleting Junos Space Network Management Platform Database Backup Files on page 614](#)
- [Backing Up and Restoring the Database Overview on page 604](#)
- [Viewing Audit Logs on page 532](#)
- [Viewing Scheduled Jobs on page 466](#)

Restoring a Database in the User Interface

You can restore any archived Junos Space Network Management Platform database to restore your Junos Space system to a previous state. When you initiate a restore database operation, Junos Space Network Management Platform is shutdown on all nodes in the fabric and the system goes into maintenance mode, during which time only one maintenance mode administrator can log in to the system at a time. Once the restore database operation is complete, Junos Space Network Management Platform is restarted and users can access the Junos Space user interface.

To restore a database, you must have System Administrator privileges and be a Maintenance Mode administrator.



NOTE: Before you restore a database, wait until all jobs currently running have completed.

To view information about the available database backup files before you select a database to restore, see [“Viewing Database Backup Files” on page 613](#).

Junos Space Network Management Platform supports both local and remote backup and restore operations.



CAUTION: The restore operation replaces the existing data with the contents of the backup file. Merging of data does not occur.

- [Restoring a Local Database on page 610](#)
- [Restoring the Database from a Remote File on page 611](#)

Restoring a Local Database

To restore the Junos Space Network Management Platform database to a previous state:

1. Select **Administration > Database Backup and Restore**.

The Database Backup and Restore page appears displaying the previous database backups.

2. Select the database backup file you want to restore.
3. Select **Restore** from the Actions menu.

The Restore confirmation dialog box appears and displays the following message:

Warning: you are about to enter maintenance mode. Space will be shutdown to restore database. All data generated after the selected backup will be lost, and other users will not be able to access the system during the operation. Do you want to continue?

4. Click **Continue** in the Restore dialog box.

Junos Space Network Management Platform prompts you to enter a username and password to enter maintenance mode.

5. Enter the maintenance mode username and password.
6. Click **OK**.

Junos Space Network Management Platform is shut down and other users will be unable to access the system during the restore database operation.

The Restore Database Status dialog box displays the status for the restore database operation.

7. In the Restore Database Status dialog box, click **Return to Maintenance Menu**.

The Maintenance Mode Actions dialog box appears.

8. In the Maintenance Mode Actions dialog box, click **Log Out and Exit from Maintenance Mode**. This action exits maintenance mode, starts up Junos Space Network Management Platform, and returns to normal operational mode.

The process of exiting maintenance mode and restarting Junos Space Network Management Platform takes several minutes.

Depending on the contents of the backup file (which might contain both network monitoring and MySQL data, or just MySQL data), either only MySQL data is refreshed, or both MySQL and network monitoring data are refreshed on the system.

Restoring the Database from a Remote File

You need to restore the Junos Space Network Management Platform database from a remote file if the device to which you are restoring it has been reimaged.

The restore operation restores the data based on the contents of the backup file. The backup file can contain both network monitoring and MySQL data, or just MySQL data.



CAUTION:

- The restore operation replaces the existing data with the contents of the backup file. Merging of data does not occur.
- The database restoration operation is performed while Junos Space Network Management Platform is in maintenance mode. During this time, all Junos Space Network Management Platform users, except the maintenance mode administrator, are locked out of the Junos Space system.

To restore a database, you must have System Administrator privileges and be a Maintenance Mode administrator.

To restore the database from a remote file:

1. Select **Administration > Database Backup and Restore** and select the **Restore From Remote File** icon.

The Restore From Remote File page appears.

2. Enter your username and password, and confirm the password, in the appropriate fields.
3. In the **Machine IP** field, enter the IP address of the device on which the backup file is located.
4. In the **File Path** field, enter the path to the backup file on that device.
5. (Optional) In the **Comment** field, enter a comment to capture any information about this database restore operation.
6. Click **Restore** to start the database restoration process.

The Restore Database confirmation dialog box appears.



WARNING: You must log in to Junos Space Maintenance mode. Junos Space Network Management Platform shuts down to restore the database. All data generated after the selected backup will be lost. Junos Space users will not be able to log in to Junos Space Network Management Platform during the restore database operation.

7. Click **Continue** in the Restore Database dialog box.

Junos Space Network Management Platform prompts you to enter a username and password to log in to the Maintenance mode.

8. Enter the maintenance mode username and password.
9. Click **OK**.

Junos Space Network Management Platform is shut down and other users will be unable to access the system during the restore database operation.

The Restore Database Status dialog box displays the status of the restore database operation.

10. In the Restore Database Status dialog box, click **Return to Maintenance Menu**.

The Maintenance Mode Actions dialog box appears.

11. In the Maintenance Mode Actions dialog box, click **Log Out and Exit from Maintenance Mode**. This action exits maintenance mode, starts up Junos Space Network Management Platform, and returns to normal operational mode.

The process of exiting maintenance mode and restarting Junos Space Network Management Platform takes several minutes.

Depending on the contents of the backup file (which might contain both network monitoring and MySQL data, or just MySQL data), either only MySQL data is refreshed, or both MySQL and network monitoring data are refreshed on the system.

- Related Documentation
- [Backing Up the Junos Space Network Management Platform Database on page 605](#)
 - [Viewing Database Backup Files on page 613](#)
 - [Deleting Junos Space Network Management Platform Database Backup Files on page 614](#)
 - [Maintenance Mode Overview on page 548](#)

Viewing Database Backup Files

The Database Backup and Restore inventory page displays information about Junos Space Network Management Platform database backups, including the date and time of the backup, the backup file name and location, and the IP address of the Junos Space Appliance that was backed up. From the Database Backup and Restore inventory page, the administrator can restore a database or delete a database backup.

- [Changing Views on page 613](#)
- [Viewing Database Details on page 613](#)
- [Manage Database Commands on page 614](#)

Changing Views

You can view database backup information in tabular view. Each database backup is represented by a row in the table.

To change views:

1. Select **Administration > Database Backup and Restore**.
The Database Backup and Restore page appears.
2. Click the **Display Quick View** icon on the Database Backup and Restore page title bar.

Viewing Database Details

To view detailed database backup information:

1. Select **Administration > Database Backup and Restore**.
The Database Backup and Restore page appears.
2. Double-click a database in the table view. The View Backup page appears.
[Table 90 on page 613](#) defines the database backup detailed information.

Table 90: Fields in the Manage Databases Table

Field	Description
Name	The name of the database backup file. Junos Space Network Management Platform automatically assigns a name to the backup file.

Table 90: Fields in the Manage Databases Table (*continued*)

Backup Date	Date and time of the database backup.
Comment	Information a Junos Space user optionally provides in the Comments field of the Backup page when scheduling database backup.
Machine	IP address of the Junos Space Appliance on which the database backup was performed.
File Path	File path for the database backup.

Manage Database Commands

From the Database Backup and Restore page, you can perform the following actions:

- Delete Database Backup—“[Deleting Junos Space Network Management Platform Database Backup Files](#)” on page 614
- Restore Database—“[Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface](#)” on page 610
- Tag It—“[Tagging an Object](#)” on page 695
- View Tags—“[Tagging an Object](#)” on page 695
- Clear All Selections—Clears all selections you made on the Database Backup and Restore page.

Deleting Database Backup Files

The system administrator can delete archived database backup files that are no longer useful for restore operations.



NOTE: When you delete a database backup file from the Database Backup and Restore inventory page, the backup file is permanently deleted from Junos Space Network Management Platform and cannot be retrieved or restored.

To delete a Junos Space Network Management Platform database backup file:

1. Select **Administration > Database Backup and Restore**.
The Database Backup and Restore page appears.
2. From the Database Backup and Restore page table view, select one or more database backup files that you want to delete.
3. (Optional) View the database backup file detailed information before deleting the file. Detailed database backup file information appears as columns in the table.
4. Click **Delete Backup**.

Junos Space Network Management Platform deletes the selected Junos Space Network Management Platform database backup files. The deleted backup files are no longer displayed in the inventory page and are deleted from the `/var/cache/jboss/backup` directory.

- Related Documentation**
- [Backing Up the Junos Space Network Management Platform Database on page 605](#)
 - [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 610](#)
 - [Viewing Database Backup Files on page 613](#)

Viewing Job Recurrence

You can view information about when a job recurs. For example, you can examine the recurrence of a database backup job.

To view job recurrence information:

1. Select **Jobs > Job Management**.

The Job Management page appears.

2. Select a recurring job and select **View Recurrence** from the Actions menu.

The View Job Recurrence dialog box displays the selected job start date and time, recurrence interval, and end date and time.

3. (Optional) Click the **Job ID** link to view all recurrences of the schedule.
4. Click **OK** on the View Job Recurrence dialog box to return to the Job Management page.

- Related Documentation**
- [Backing Up the Junos Space Network Management Platform Database on page 605](#)
 - [Viewing Scheduled Jobs on page 466](#)
 - [Viewing Audit Logs on page 532](#)

Manage Licenses

- [Generating and Uploading the Junos Space License Key File on page 617](#)
- [Viewing Licenses on page 619](#)

Generating and Uploading the Junos Space License Key File



NOTE:

- From Junos Space Network Management Platform Release 13.1R1 onward, the licensing model of Junos Space does not require license keys for Junos Space applications. However, a license file is still needed for the Junos Space Platform functionality because the default Junos Space Platform license file is valid only for 60 days after which the Junos Space Platform functionality is not available.

When you purchase a commercial version of Junos Space Platform, Juniper Networks provides you with a license file that does not have any expiry date. After you import this license into Junos Space Platform, you have access to the full Junos Space Platform functionality for an unlimited period.

- Since Junos Space applications do not use license keys, the Licenses page (Administration > Licenses) does not display licensing information for any Junos Space applications that you might have purchased and installed. However, if you use Junos Space Platform with only Service Now and Service Insight installed, licensing information for those applications is displayed on the Licenses page. To find out the licensing information about Junos Space applications that you purchased, please contact the Juniper Technical Assistance Center.

The Junos Space Network Management Platform software provides a default, 60-day trial license. After 60 days, the use of the Junos Space Network Management Platform software expires except for the **Import License** action. The administrator must activate the software with the Juniper Networks license key to regain use of the Junos Space Platform. Two weeks before the license expiration date, a license expiration warning appears when users log in to Junos Space Platform.

Junos Space Network Management Platform license management involves a two-step process:

1. Generating the license key file. Juniper Networks uses a license management system (LMS) to manage the deployment of the Junos Space Network Management Platform product—appliances, connection points, connections, and applications. When you order Junos Space Network Management Platform, the Juniper Networks LMS sends you an e-mail with an authorization code and a software serial number and instructions on how to generate a license key.
2. Import the license key into Junos Space Platform. The system administrator must import the Junos Space license key file from the Licenses page (**Administration > Licenses**) to use Junos Space Platform beyond the trial period.

This procedure includes the following topics:

1. [Generating the License Key File on page 618](#)
2. [Uploading the License Key File Contents on page 618](#)

Generating the License Key File

When you order Junos Space Platform, Juniper Networks sends an e-mail containing an authorization code and a software serial number (the serial number that identifies the software installation) along with instructions on how to generate the license key.

When you order a Junos Space Appliance, Juniper Networks sends an e-mail containing the serial number for the appliance that is licensed for the appropriate stock-keeping unit (SKU).

Uploading the License Key File Contents

To upload the license key file, follow these steps:

1. Open the Juniper Networks Authorization Codes e-mail you received and follow the directions.
2. Open the license key text file attached to the e-mail and copy all the contents.
3. In the Junos Space Platform UI, select **Administration > Licenses**.

The Licenses page appears.

4. Click the **Import License** icon.

The Import License page appears.

5. Paste the contents of the license key text file in the License data text field using the Web browser Edit > Paste command.

6. Click **Upload**.

The license key data is uploaded to the Junos Space Platform database. A message indicating that the Junos Space license is uploaded successfully appears.

7. Click **OK**.

The Junos Space license appears on the Licenses inventory page.

**Related
Documentation**

- [Viewing Licenses on page 619](#)

Viewing Licenses



NOTE: From Junos Space Network Management Platform Release 13.1R1 onward, the licensing model of Junos Space does not require license keys for Junos Space applications. However, a license file is still needed for the Junos Space Platform functionality because the default Junos Space Platform license file is valid only for 60 days after which the Junos Space Platform functionality is not available.

Since Junos Space applications do not use license keys, the Licenses page (Administration > Licenses) does not display licensing information for any Junos Space applications that you might have purchased and installed. However, if you use Junos Space Platform with only Service Now and Service Insight installed, licensing information for those applications is displayed on the Licenses page. To find out the licensing information about Junos Space applications that you purchased, please contact the Juniper Technical Assistance Center.

The Licenses inventory page displays the Junos Space Platform license that the administrator has uploaded. For more information about obtaining and uploading the Junos Space Platform license, see [“Generating and Uploading the Junos Space License Key File” on page 617](#).

The Licenses page displays the Junos Space Network Management Platform trial license until you upload the one specifically generated for your software installation.

- [Viewing License Details on page 619](#)

Viewing License Details

In the table, you see the following license detailed information.

[Table 91 on page 619](#) defines the license details.

Table 91: Licenses Details

Field	Description
-------	-------------

Table 91: Licenses Details (*continued*)

License Type	The Junos Space Platform license can either be a trial license installed (Trial) with the Junos Space Platform software image or a commercial one (Commercial) that you upload into Junos Space Platform.
Sku Model #	The Junos Space Network Management Platform license stock-keeping unit (SKU) model number. If the license is a trial license, the SKU displayed is Trial-license . If it is a commercial license, the license SKU is displayed; for example, JS-PLATFORM .
Total License Days	For a trial license, the total number of license days is 60. For a commercial license, the total number of license days is unlimited (Unlimited).
Remaining License Days	For a trial license, the remaining number of days is the countdown of the number of days since you installed Junos Space Platform (for example, 36). For a commercial license, the remaining number of days is unlimited (Unlimited).

**Related
Documentation**

- [Junos Space User Interface Overview on page 9](#)
- [Exporting License Inventory on page 80](#)

CHAPTER 64

Manage Applications

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)
- [Modifying Application Settings on page 624](#)
- [Modifying Network Application Platform Settings on page 626](#)
- [Configuring Password Settings on page 628](#)
- [Managing Services on page 631](#)
- [Configuring Network Activate Application Settings on page 634](#)
- [Adding a Junos Space Application on page 635](#)
- [Junos Space Software Upgrade Overview on page 637](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Upgrading Junos Space Software Overview on page 639](#)
- [Upgrading Junos Space Network Management Platform on page 641](#)
- [Uninstalling a Junos Space Application on page 646](#)

Application Management Overview

You can use the Applications pages to manage the Junos Space Network Management Platform (platform) and all other separately packaged applications.

In these pages, you can perform the following tasks:

- Install new Junos Space application using the **Administration > Applications > Add Application** task, see [“Adding a Junos Space Application” on page 635](#).
- Upgrade the Junos Space Network Management Platform using the **Administration > Applications > Upgrade Platform** action, see [“Upgrading Junos Space Network Management Platform” on page 641](#). The Junos Space Network Management Platform provides the running environment for all Junos Space applications, so upgrading it causes operation interruption.
- Upgrade a Junos Space application while Junos Space Network Management Platform is still running using the **Administration > Applications > Upgrade Application** action, see [“Upgrading a Junos Space Application” on page 638](#).

- Uninstall a Junos Space application while Junos Space Network Management Platform is still running using the **Administration > Applications > Uninstall Application** action, see [“Uninstalling a Junos Space Application” on page 646](#).
- Modify application settings using the **Network Management Platform > Administration > Applications > Modify Application Settings** action, see [“Modifying Junos Space Application Settings” on page 624](#).
- Start, stop, or restart services using the **Administration > Applications > Manage Services** action, see [“Managing Services” on page 631](#).
- Tag applications to categorize them for filtering and performing Manage Applications actions using the **Administration > Applications > Tag It** action, see [“Tagging an Object” on page 695](#).
- View tags that you have already created on a selected application using the **Network Management Platform > Administration > Applications > View Tags** action, see [“Viewing Tags for a Managed Object” on page 696](#).



NOTE: The Junos Space Network Management Platform Upgrade image includes the Junos Space Network Management Platform, Service Now, and Service Insight. Other Junos Space applications are separately packaged in image files. The administrator must download application files from the Juniper Networks Web site to the local client file system. The administrator must upload an application file in Junos Space Network Management Platform. Once uploaded, Junos Space installs or upgrades the application. When the application is installed, you can launch it from Application Chooser. When you upgrade Junos Space Network Management Platform, all applications except Service Now are disabled. Upgrade all disabled applications to the current release. Users in an upgraded application's workspace are directed to Application Chooser.

Related Documentation

- [Managing Junos Space Applications on page 622](#)
- [Modifying Junos Space Application Settings on page 624](#)
- [Uninstalling a Junos Space Application on page 646](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Upgrading Junos Space Network Management Platform on page 641](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)

Managing Junos Space Applications

Manage Junos Space applications from the **Administration > Applications** task. All applications that you have uploaded and installed appear in the **Applications** inventory page. From the Manage Applications inventory page you, the super administrator or

system administrator can manage Junos Space hot-pluggable applications, such as install, upgrade, and uninstall, while Junos Space Network Management Platform is still running. You can also upgrade the Junos Space Network Management Platform that provides the runtime environment for all Junos Space Network Management Platform applications. Upgrading the Junos Space Network Management Platform causes an interruption of Junos Space Network Management Platform operation. The Junos Space Network Management Platform upgrade takes place in Maintenance mode.

The administrator can also modify Junos Space Network Management Platform application settings and tag applications to categorize and filter them to perform bulk actions on multiple applications at once.

- [Installing or Upgrading an Application on page 623](#)
- [Viewing Detailed Application Information on page 623](#)
- [Performing Manage Application Actions on page 624](#)

Installing or Upgrading an Application

To install or upgrade an application:

1. Download a new Junos Space application from the Juniper Networks software download site to the local client machine
2. To add an application, upload that application into Junos Space Network Management Platform using **Administration > Applications** and the Add Application icon. To upgrade an application, select **Administration > Applications**. Select the application on the Applications inventory page, then select **Upgrade Application** from the Actions menu.
3. Once uploaded, you can install or upgrade the application.
4. Once you upgrade or install an application, it appears on the Manage Applications inventory page. The new or upgraded application appears in Application Chooser and the Application Switcher global action pop-up menu at the right in the Application Chooser title bar.

Viewing Detailed Application Information

[Table 92 on page 623](#) defines the information displayed in table columns for each application in the Manage Applications inventory page.

Table 92: Application Information

Application Information	Description
Title	Name of the Junos Space application.
Version	The Junos Space application software version.
Release Type	The Junos Space application software version release level.
Build	The Junos Space application software build number.

Performing Manage Application Actions

You can perform the following actions on applications from the Manage Applications Actions menu. You must first select an application before you can perform an action on it from the Actions menu. You can also right-click an application to perform these actions.

- Modify Application Settings—See “[Modifying Junos Space Application Settings](#)” on [page 624](#).



NOTE: This action is available for Junos Space Network Management Platform only.

- Uninstall Application—See “[Uninstalling a Junos Space Application](#)” on [page 646](#).
- Upgrade Application—See “[Upgrading a Junos Space Application](#)” on [page 638](#).
- Upgrade Platform—See “[Upgrading Junos Space Network Management Platform](#)” on [page 641](#).



NOTE: This action is available for Junos Space Network Management Platform only.

- Tag It—See “[Tagging an Object](#)” on [page 695](#).
- View Tags—See “[Viewing Tags for a Managed Object](#)” on [page 696](#).
- Untag It—“[Untagging Objects](#)” on [page 697](#).

Modifying Application Settings

You, the Super Administrator or System Administrator, can modify Junos Space application settings.

To modify application settings:

1. Select **Administration > Applications**.

The **Applications** inventory page appears.

2. Select the application.

Select Network Management Platform to modify the Junos Space Network Management Platform application settings.

3. Select **Modify Application Settings** from the Actions menu.

The appropriate Modify Network Management Platform Settings page appears.

4. Configure the following application settings depending on the application you are managing:
 - [Modifying Network Management Platform Settings on page 626](#)
 - [Configuring Network Activate Application Settings on page 634](#)
5. Click **Modify**.



NOTE: You cannot modify the application settings if another user is currently modifying the application settings. You will receive a pop-up message indicating the user who is currently modifying the application settings.



NOTE: We recommend that you do not navigate to other pages or other Junos Space applications when modifying the application settings. Save the changes before you navigate to other pages or other Junos Space applications.

**Related
Documentation**

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)
- [Uninstalling a Junos Space Application on page 646](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Creating a Tag on page 698](#)
- [Managing Tags on page 688](#)

Modifying Network Application Platform Settings

Table 93 on page 626 lists the application settings you can configure for Junos Space Network Management Platform. You must have super administrator or system administrator privileges.

Table 93: Junos Space Network Management Platform Application Settings

Category	Parameter Label	Description
Device	Add SNMP configuration during device discovery	<p>This check box is selected by default and ensures that the SNMP target for the devices that are discovered from Junos Space Network Management Platform is set to the Junos Space VIP node. This configuration enables these devices to send their SNMP traps to the Junos Space VIP node.</p> <p>If you clear the check box, then SNMP trap targets are not set for the devices that are newly added in Junos Space Network Management Platform. The devices whose SNMP trap targets are not set do not send their SNMP traps to the Junos Space VIP node.</p>
	Allow users to auto log in to devices using SSH	This check box allows users to automatically log in when starting an SSH connection on a device. The default, deselected, indicates that you have to add your credentials to log in to a device using SSH.
	Auto resync device	This check box ensures that when the network is the system of record, configuration changes on a connected Juniper Networks device are synchronized, or imported, to the application database. By default this check box is selected.
	Configure commit synchronize during device discovery	This check box ensures that for either system of record, configuration changes in Junos Space Network Management Platform for a device are pushed, committed, and synchronized during device discovery.
	Junos Space Network Management Platform initiates connection to device	This check box is selected by default, so Junos Space Network Management Platform initiates connection with managed devices. To have managed devices initiate connection with Junos Space Network Management Platform, deselect this check box.
	Max auto resync waiting time secs	This field specifies the time within which device configuration changes are synchronized to the database. The default waiting time is 20 seconds. You can specify any number of seconds. There is no specific range. This setting applies only when the network is the system of record.
	Number of Devices to connect per minute for Space Initiated Connection	This parameter enables you to throttle the number of devices that connect to Space. Having thousands of devices trying to connect simultaneously impacts performance negatively. The default number of devices allowed to connect per minute in connections initiated by Junos Space Network Management Platform is 500 devices.
	Polling time period secs	This setting is for specifying the interval at which to poll the configuration of devices that do not support system logging. Junos Space Network Management Platform polls and compares the configuration it has with that of the device(s) at the interval set here. If there is a difference, it is reported. If the network is the system of record, Junos Space Network Management Platform synchronizes its configuration. The default is 900 seconds.
	SSH port for device connection	

Table 93: Junos Space Network Management Platform Application Settings (*continued*)

Category	Parameter Label	Description
		This text field specifies the SSH port on the device. Junos Space Network Management Platform uses this port to discover devices. The default value, 22, is the standard SSH server port.
	Support WW Junos devices	This check box enables you to manage devices running the worldwide version of Junos OS (ww Junos OS devices) through Junos Space Network Management Platform.
	Space as system of record choices	<p>This setting specifies whether the network is the system of record (NSOR, the default) or Junos Space Network Management Platform is the system of record (SSOR).</p> <p>NOTE: Resynchronization choices in this page apply only to NSOR.</p> <p>See also “Systems of Record in Junos Space Overview” on page 733.</p>
User	Automatic logout after inactivity (minutes)	<p>This field specifies the time, in minutes, after which a user who is idle and has not performed any action, such as keystrokes or mouse clicks, is automatically logged out of Junos Space Network Management Platform. This setting conserves server resources and protects the system from unauthorized access.</p> <p>By default, the user is logged out if the user is inactive for 5 minutes. If you set the configuration to Never, the user is never logged out of Junos Space Network Management Platform due to inactivity.</p>
	Maximum concurrent UI sessions per user	<p>This text box specifies the number of concurrent user sessions allowed per user for GUI login at global level (that is, for all users).</p> <p>The default value is 5. You can enter a value from 0 through 999. Entering 0 (zero) means that there are no restrictions to the number of concurrent UI sessions allowed per user. However, the system performance maybe degraded if you allow unlimited concurrent UI sessions.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you are a super user, this concurrent user session limit does not apply and you are allowed to log in even when you have exceeded this limit. • The changes that you do to the concurrent UI sessions limit (either at the global-level or at the user-level) do not impact the existing sessions. That is, this limit is validated against the next user log in only. <p>For more information, see “Limiting User Sessions” in “Creating User Accounts” on page 509.</p>
	Use User Password Auth Mode choices	<ul style="list-style-type: none"> • Use User Password Auth Mode—Select for the Junos Space server to authenticate the user based on the username and password entered by the user. • Use X509 Certificate Auth Mode—Select for the Junos Space server to authenticate the user based on the certificate of the user.
Password	See “Configuring Password Settings for Junos Space Network Management Platform” on page 628 .	
Audit Log	Record HTTP GET method	This check box audit logs all API GET calls.

Table 93: Junos Space Network Management Platform Application Settings (*continued*)

Category	Parameter Label	Description
Search	Index auto update interval in seconds	By default, the value for this field is set to five seconds, which means that for every five seconds the system automatically checks whether there are any new changes in the database that needs to be indexed.
	Pause indexing during device import	If you have to discover large number of devices (for example, in the range of thousands), this setting speeds up the device discovery approximately by 10%.

Related Documentation

- [Modifying Junos Space Application Settings on page 624](#)
- [Configuring Password Settings for Junos Space Network Management Platform on page 628](#)
- [Worldwide Junos OS Adapter Overview on page 165](#)
- [Systems of Record in Junos Space Overview on page 733](#)

Configuring Password Settings

Beginning with Junos Space Network Application Platform Release 12.1, Junos Space Network Management Platform has implemented a default standard for passwords that is compliant with industry standards for security.



NOTE: If you are upgrading to Space Platform Release 12.1 or later, these default password settings take effect immediately. All local users will get password expiration messages the first time they log in after the upgrade.

Users go to User Preferences (see “[Changing Your Password on Junos Space](#)” on page 4) to create new passwords, but the constraints that govern those passwords are set in the Administration workspace. This topic describes the parameters that limit password creation and how to set them.

Users creating their passwords can view the parameters set by the Junos Space administrator. To display the rules, users can click the Help icon next to the password field on both the Create User page and the User Preferences - Change Local Password and Certificate page.

To configure password settings:

1. Select **Administration > Applications**.

The Applications inventory page appears.

2. Select **Network Management Platform**, and select **Modify Application Settings** from the Actions menu.

The Modify Network Management Platform Settings page appears.

3. To configure the password settings, click **Password**.

The Password page appears.

[Table 94 on page 629](#) describes all the parameters for password rules.

Table 94: Password Constraint Parameters

Parameter	Default (yes, no, or default value)	Explanation or Example
Minimum no. of characters	6	<p>The value entered here determines the minimum number of numbers, letters, and special characters permitted.</p> <p>The minimum value for this field is 6 and the maximum value is 999.</p>
No. of previous passwords cannot be reused	6	<p>The value entered here determines how 'old' passwords must be before users are allowed to reuse them. Entering 10 means that users cannot reuse any of the last 10 Junos Space Network Management Platform passwords they have had. Entering 1 means that users cannot reuse their last password, but can use their second-to-last password. Entering 0 means that users can reuse even their last passwords. You can enter a value from 0 through 999.</p> <p>Typically, a password is validated against this constraint when the user tries to modify the password.</p>
No. of unsuccessful attempts before logout	4	<p>Junos Space Network Management Platform locks out users who enter more than the permitted number of incorrect passwords defined here. The system identifies users by their IP addresses, so that even if users have exceeded the limit for incorrect passwords on one machine, they can try to log in again from a different machine.</p> <p>You can enter a value from 0 through 999. Entering 0 means that users are not locked out due to login failures. Because the users are not locked out, the users can try to login multiple times from the same IP address.</p> <p>NOTE: This verification applies only to users who are in the Junos Space Network Management Platform database. It does not work with Radius and TACACS authentication.</p>
Time interval for logout in hours	12	<p>A user who has entered too many incorrect passwords is locked out for the amount of time defined here in hours.</p> <p>You can enter a value from 0 through 999. Entering 0 means that users are never locked out even if they are unable to login due to wrong user credentials.</p> <p>For example, if you have set the "No. of unsuccessful attempts before logout" to 2 and "Time interval for logout in hours" to 0, then the user can log in at the 3rd attempt.</p> <p>NOTE: You can reenable a locked out user at any time (see "Disabling and Enabling Users" on page 515)</p>

Table 94: Password Constraint Parameters (*continued*)

Parameter	Default (yes, no, or default value)	Explanation or Example
Time interval for password expiry in months	3	<p>The value entered here determines the duration after which the passwords of all the Junos Space Network Management Platform locally authenticated users will expire. Entering 10 means that the passwords of all the users expire after duration of 10 months from the time you made this change. Entering 0 means that the passwords never expire. You can enter a value from 0 through 999.</p> <p>When new users are added locally or when the existing users change their passwords, the password expiry time of these users are set to the configured value. The default value is 3 months, which means that the passwords of these users expire after three months.</p> <p>NOTE:</p> <ul style="list-style-type: none"> This configuration does not have any impact on the RADIUS or TACACS server authenticated users. If you upgrade to Junos Space Release 13.1 or later, the password expiry time of the existing local users remain as is until the users modify their passwords or you change the value in this field.
Time interval for password expiry notification in months	1	<p>The value entered here determines the number of months in advance users are warned that their passwords will expire. If you enter 2, two months before users' current passwords expire, they receive a notification that they must change their passwords.</p> <p>You can enter a value from 0 through 999. Make sure that the value you enter here is less than or equal to the password expiry time (that is, this value should be less than or equal to the value in the "Time interval for password expiry in months" text box). Else, Junos Space Network Management Platform throws the following error message: "Time interval for password expiry notification in months value should be less than or equal to Time interval for password expiry in months."</p>
Click the view/configure link next to Advanced Settings to display the following fields:		
At least one lowercase character	yes	Enabling this check box means that EXAMPLE is permissible, and so is example , but EXAMPLE is not permissible.
At least one number not in the last position	yes	Enabling this check box means that examp2e is permissible, and so is 2example , but example2 is not permissible.
At least one special character not in the last position	no	Enabling this check box means that examp\$e is permissible, and so is \$example , but example\$ is not permissible.
At least one uppercase character	no	Enabling this check box means that Example is permissible, and so is EXAMPLE , but example is not permissible.
No more than three repetitive characters	yes	Enabling this check box means that users are not allowed to create passwords by simply adding a single character multiple times. It means that example111 or exampleee is permissible, and so is 1example1 or eexample , but 11example11 is not permissible, nor is eexampleee .

Table 94: Password Constraint Parameters (*continued*)

Parameter	Default (yes, no, or default value)	Explanation or Example
Not repeat of the user ID	yes	Enabling this check box prevents users from using their IDs as passwords. For example, someone with the username <i>johndoe</i> would not be allowed to have the password johndoe .
Not reverse of the user ID	yes	Enabling this check box prevents users from reversing their IDs to use as passwords. For example, someone with the username <i>johndoe</i> would not be allowed to have the password doejohn .

4. Make your settings as desired, using [Table 94 on page 629](#) for guidance.

5. Click **Modify** to apply your choices.

For troubleshooting, see the `/var/log/jboss/server.log` file, which captures any internal errors. Also, see the audit logs, which captures the configuration changes that you perform on the Password page.

Related Documentation

- [Disabling and Enabling Users on page 515](#)
- [Creating User Accounts on page 509](#)
- [Application Management Overview on page 621](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Modifying Junos Space Application Settings on page 624](#)

Managing Services

This topic describes how to start, stop, and restart Network Monitoring (that is, the network monitoring services). Currently, Network Monitoring is the only service that can be managed this way.

Service management operations—start, stop, restart—are applied on all the nodes that run the service.

The service management actions generate audit log entries.

The Super Administrator and System Administrator predefined roles have the permissions to manage services; the corresponding action is Manage Services. If a user does not have a role that includes this action, the Manage Services option is not available.

The following table describes the consequences of performing these three actions:

Table 95: Starting, Stopping, and Restarting Network Monitoring

Action	Consequences
Stop	Network Monitoring service is stopped on all nodes.
	Even if VIP failover is performed, service remains stopped on all nodes.
	The syncing of network monitoring data is disabled.
	Even after adding a new node, the network monitoring service remains stopped.
	Rebooting Junos Space Network Management Platform does not restart a service.
Start, Restart	Network Monitoring service starts only on the VIP node.
	All the devices displayed on the Devices page are discovered by the network monitoring functionality. The SNMP trap targets are correct.
	All the users displayed on the Users page are added to network monitoring.
	Email and remote server settings are added to network monitoring.
	All Junos Space nodes are monitored by the network monitoring functionality.
Start, Stop, Restart when no service is selected	Service remains up and running even if Junos Space Network Management Platform is rebooted.
	Error message is displayed: No service selected.



NOTE: The following firewall ports should be closed on stopping the network monitoring service:

- UDP
 - 162
 - 514
 - 5813
- TCP
 - 5813
 - 18980



NOTE: Any devices added while the Network Monitoring service is stopped must be manually resynchronized from the Network Monitoring workspace after the service is restarted.

To start, stop, or restart network monitoring services:

1. Select **Administration > Applications**.

The Applications inventory page appears.

2. Do either of the following:

- Select **Network Management Platform** and select **Manage Services** from the Actions menu.

The Manage Services page appears, showing the names of the services that can be managed this way (currently Network Monitoring is the only item in this list), and the Start, Stop, and Restart buttons, as well as a table displaying the following information:

Column Heading	Content
Service Name	Name of service capable of being started, stopped or restarted
Running Version	Version of the service that is currently running
Status	Current status: Enabled or Disabled

3. Select **Network Monitoring** from the list, and select the relevant button for a currently enabled service: **Start**, **Restart** or **Stop**.

One of four messages appears:

- If you select a service that is currently running, then select **Stop**, you will receive this message:

Confirm Stop Service: Do you really want to stop the service?

- If you select a service that has been disabled, then select **Restart**, you will receive this message:

Warning: Sorry, cannot proceed with the request, as the Service is not in Enabled state.

- If you select a service that has been disabled, then select **Start**, you will receive this message:

Warning: Sorry, Network Monitoring cannot be started once it is stopped.

- If you select a service that has been disabled, then select **Stop**, you will receive this message:

Warning: Sorry, cannot proceed with the request, as the Service is already in Disabled state.

4. In all cases, you can only select **OK**.

First a message appears, announcing that the relevant action is being performed, and then a second status message, announcing that the operation you performed was successful—or not.

5. Select **OK** to confirm.

The Manage Services page reappears, displaying the selected service's changed status.

Related Documentation

- [Application Management Overview on page 621](#)
- [Junos Space Audit Logs Overview on page 531](#)
- [Role-Based Access Control Overview on page 479](#)

Configuring Network Activate Application Settings

You can configure the Network Activate application settings from the Administration > Applications inventory page. See "[Modifying Junos Space Application Settings](#)" on page 624

You must have Super Administrator privileges to configure Network Activate application settings.

[Table 96 on page 634](#) defines the application settings you can configure for the Network Activate application settings.

Table 96: Network Activate Application Settings

Category	Application Setting Name	Description
Deployment	Deploy configuration to the device	Disable this setting to deploy configuration to Junos Space Network Management Platform user interface only.
	Save configuration in XML format	This setting is disabled by default, to deploy the service order and view the configuration using JUNOS curly braces syntax.
	Use vlanmaps for flexible tagged services	Enable this setting if MX Series devices are configured for VLAN mapping.
Audit	Perform functional audit on control plane only	Enable this option to check only the control plane to ensure connectivity among endpoints and verify that UNIs are functioning correctly. Disable this setting to check the control plane and also the data plane to verify packet transmission between each valid pair of endpoints in the service.
Logging	Log Directory	Modify the default audit log repository directory. The default log directory is <code>/var/tmp/jboss</code> .

Related Documentation

- [Modifying Junos Space Application Settings on page 624](#)

Adding a Junos Space Application

The administrator can add a new Junos Space application while Junos Space Network Management Platform is still running.



NOTE: Service Now and Service Insight are bundled with, installed, and upgraded with Junos Space Network Management Platform. You must add, or upgrade all other applications separately.

To upgrade Junos Space applications, see “[Upgrading a Junos Space Application](#)” on [page 638](#).

Adding an application to the Junos Space Network Management Platform server is a two-step process:

1. Upload the application to the Junos Space Network Management Platform server.
2. Install the uploaded application.

To upload a Junos Space application:

1. Ensure that the Junos Space application you want to add is downloaded from the Juniper Software download site to the local client file system.

<https://www.juniper.net/support/products/space/#sw>

2. Select **Administration > Applications** and select the Add Application icon.

The Add Application page appears. If you have not uploaded any applications, the page is blank.

3. Upload the new application by performing one of the following:
 - a. Click **Upload via HTTP**.

The Software File dialog box appears.

- i. Type the name of the application file or click **Browse** to navigate to where the new Junos Space application file is located on the local file system.
- ii. Click **Upload**. This action might take a while. Wait until the application is uploaded.

If you are trying to upload an application that is not supported by Junos Space Network Management Platform Release 13.1, then Junos Space Network Management Platform displays the following error message:

Current platform version does not support this software version.

The Application Management Job Information dialog box appears. Go to step [4](#) to confirm whether the application is uploaded successfully.

- b. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. Add the Secure Copy credentials to upload the Junos Space Network Management Platform application image from a remote server to Junos Space.

- i. Enter your username.
- ii. Enter your password.
- iii. Enter your password again to confirm the password.
- iv. Enter the host IP address.
- v. Enter the path name of the Junos Software application file.

For example, `/root/<image-name>.img`.

- vi. Click **Upload**. This action might take a while. Wait until the application is uploaded.

If you are trying to upload an application that is not supported by Junos Space Network Management Platform Release 13.1, then Junos Space Network Management Platform displays the following error message:

Current platform version does not support this software version.

The Application Management Job Information dialog box appears. Go to step 4 to confirm whether the application is uploaded successfully.

4. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the **Jobs > Job Management** inventory page. Wait until the job is completed and ensure that the job is successful.

If the upload is successful, then the new application is displayed by application name, filename, version, release level, and the required Junos Space Network Management Platform version on the Add Application page.

To install the uploaded application:

1. Select **Administration > Applications > Add Application** icon.

The Add Application page appears.

2. Select the uploaded application.
3. Click **Install**.

The Application configuration page appears.

4. Click **OK** to proceed.

The Application Management Job Information dialog box appears.

5. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the **Jobs > Job Management** inventory page. Wait until the application is fully deployed and ensure that the job is successful.

If the installation is a failure, the Summary column for the job displays the reasons, if any, for the installation failure. For example, you must have successfully installed

Network Activate before installing Transport Activate. If you try to install Transport Activate without Network Activate, the following error message is thrown: **Network Activate is not installed. Transport Activate cannot be installed without Network Activate.** Typically, such messages are displayed for applications that are supported from Junos Space Network Management Platform Release 13.1. However, it is also dependent on the type and version of the application being installed.



NOTE: It is important that you install the applications in the right order: from the primary application to the dependent applications.

6. If the installation is successful, without logging out of Junos Space Network Management Platform, select the application from the Application Chooser list (located at the top-left) to view and begin using its workspaces and tasks.

Related Documentation

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Upgrading Junos Space Network Management Platform on page 641](#)
- [Modifying Junos Space Application Settings on page 624](#)
- [Uninstalling a Junos Space Application on page 646](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)

Junos Space Software Upgrade Overview

To upgrade software for the Junos Space Virtual Appliance, you upload the Junos Space Network Management Platform image file to your existing fabric and perform the software upgrade in the Junos Space user interface. When you perform an upgrade, all appliances (nodes) in the fabric are upgraded with the new software.

To ensure a successful upgrade of your Junos Space appliances, complete the following tasks.

- Back up all your Junos Space Network Management Platform data files before you begin the upgrade process.
- Download the Junos Space Network Management Platform software image from the Juniper Networks software download Web site.
- Complete the steps to upgrade your current Junos Space Network Management Platform software to the latest software version.



NOTE: To perform a Junos Space Network Management Platform upgrade, you must have super administrator or system administrator access privileges.

- Validate that the software is successfully installed by logging in to the user interface.

To view the version of the installed Junos Space Network Management Platform software, select the Help icon in the user interface banner and click **About**.

**Related
Documentation**

- [Upgrading Junos Space Software Overview on page 639](#)

Upgrading a Junos Space Application

The Upgrade Application action allows you to upgrade an existing Junos Space application independently while the system is still running. Several hot-pluggable Junos Space applications are available for upgrade to the current release. Once the application is upgraded successfully, you can launch it from Application Chooser.

To install a new Junos Space application, use the **Administration > Applications > Add Application** action, see [“Adding a Junos Space Application” on page 635](#).

To upgrade an existing Junos Space application:

1. Ensure that the application to which you want to upgrade is downloaded from the Juniper Software download site to the local client file system.

<https://www.juniper.net/support/products/space/#sw>

2. Select **Administration > Applications**. The Applications inventory page appears.
3. Select the application that you want to upgrade and select **Upgrade Application** from the Actions menu.

The Upgrade Application dialog box appears displaying all previously uploaded versions of that application.

4. Do one of the following:

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

The application upgrade process begins. Go to the next step.

- If the application to which you want to upgrade is not listed in the Upgrade Application dialog box, click **Upload**. The Software File dialog box appears.

- a. Click **Browse** and navigate to where the software file to which you want to upgrade is located on the local file system.

- b. Click **Upload**.

The software file is uploaded into Junos Space Network Management Platform. You see the application in the Upgrade Applications dialog box.

- c. Wait until the job is completed.

The Upgrade Application Job Information dialog box appears.

- d. Click the **Job ID** link to see the Upgrade Application job in the Manage Jobs inventory page. Review the job to:
 - i. Ensure that the job is successful.
 - ii. Select **Administration > Applications** to continue with the upgrade application process.

The Upgrade Application dialog box appears.

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

5. Navigate to the Application Chooser and launch the application you upgraded.

Related Documentation

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)
- [Adding a Junos Space Application on page 635](#)
- [Upgrading Junos Space Network Management Platform on page 641](#)
- [Modifying Junos Space Application Settings on page 624](#)
- [Uninstalling a Junos Space Application on page 646](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)

Upgrading Junos Space Software Overview

To upgrade the Junos Space Network Management Platform software, you must first download the Junos Space Network Management Platform Upgrade image file from the Juniper Networks software download site onto the local client file system. When you perform an upgrade, all appliances (nodes) in the fabric are upgraded with the new software.



CAUTION: Junos Space Network Management Platform 13.1 supports upgrading from 12.3 or 12.2. Versions prior to 12.1 may require a two-step upgrade. For example, upgrading to 13.1 from 11.4 requires that you upgrade from 11.4 to 12.2 and from 12.2 to 13.1.

- [Junos Space 13.1 Release Highlights on page 640](#)
- [Before You Begin on page 640](#)
- [Upgrading Junos Space Release to Release 13.1 and Later Versions on page 641](#)

Junos Space 13.1 Release Highlights

The Junos Space Network Management Platform Upgrade Release 13.1 includes:

Junos Space Network Management Platform Release 13.1 Contents

- Network Management Platform Release 13.1—The platform provides the operating environment for Junos Space Network Management Platform. Upgrade using the **Network Management Platform > Administration > Applications > Upgrade Platform** action.
- Service Now Release 13.1
- Service Insight Release 13.1

Available Hot-Pluggable Applications

The following applications are hot-pluggable in Junos Space Network Management Platform. Hot-pluggable applications mean that adding, removing, and upgrading occurs while Junos Space Network Management Platform is still running, and without service interruption. A hot-pluggable application is packaged separately and has a separate image file for installing and upgrading.

- Junos Space Services Activation Director—It is a suite of applications containing:
 - Network Activate
 - Transport Activate
 - QoS Design
 - Sync Design
 - OAM Insight
- Junos Space Content Director
- Junos Space Security Director
- Network Director
- Virtual Control

Before You Begin

Before you upgrade the Junos Space Network Management Platform Software, ensure that you are aware of the following:

- Upgrading to Junos Space Network Management Platform release 13.1 clears existing user preferences set using the User Preferences global action icon at the right in the title bar of Application Chooser.
- We recommend that you:
 - Back up the Junos Space Network Management Platform database before you begin the upgrade process. See also [“Application Management Overview” on page 621](#).

- Clear the Web browser cache before logging in to the upgraded Junos Space Network Management Platform software.
- You must log in as the default super administrator or system administrator to upgrade Junos Space Network Management Platform.

Upgrading Junos Space Release to Release 13.1 and Later Versions

The Platform provides the running environment for all Junos Space applications, so upgrading it causes operation interruption.



NOTE: When upgrading Junos Space Network Management Platform to 13.1 or later versions, only Network Management Platform, Service Now, and Service Insight applications are upgraded. Only the applications that are supported with Junos Space Network Management Platform Release 13.1 are enabled. Other applications running on Junos Space Network Management Platform with releases prior to 13.1 and that are not supported with Junos Space Network Management Platform Release 13.1 might be disabled. You must upgrade these disabled applications to release 13.1. (see [“Upgrading a Junos Space Application” on page 638](#)) or uninstall them (see [“Uninstalling a Junos Space Application” on page 646](#)). Do not add disabled Junos Space applications using Platform > Administration > Applications > Add Application.

To upgrade Junos Space Network Management Platform from release 12.3 or 12.2 to release 13.1, see [“Upgrading Junos Space Network Management Platform” on page 641](#).

Related Documentation

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)

Upgrading Junos Space Network Management Platform

The Junos Space Network Management Platform provides the running environment for all Junos Space applications, so upgrading causes operation interruption. The Upgrade Network Management Platform action allows the administrator to upgrade the Network Management Platform independently from one version to another without installing other Junos Space applications.



NOTE: Junos Space Network Management Platform supports upgrades from the last two versions. Junos Space Network Management Platform 13.1 supports upgrading from 12.3 or 12.2. Versions prior to 12.1 may require a two-step upgrade. For example, upgrading to 13.1 from 11.4 requires that you upgrade from 11.4 to 12.2 and from 12.2 to 13.1.



NOTE: When you perform an upgrade to Junos Space Network Management Platform release 13.1 on a single- or multi-node fabric, the installation status is shown during the installation process.

To upgrade the Junos Space Network Management Platform:

1. Ensure that the Junos Space Network Management Platform Upgrade image to which you want to upgrade is downloaded to the local client file system from the <https://www.juniper.net/support/products/space/#sw> website.

2. Select **Platform > Administration > Applications**.

The Applications inventory page appears.

3. Select the **Network Management Platform** application and select **Upgrade Platform** from the Actions menu.

The **Upgrade Platform** page appears displaying all previously uploaded versions of the Junos Space Network Management Platform image.

4. Do one of the following:

- If the release to which you want to upgrade is listed on the Upgrade Platform page, select the file, and click **Upgrade**.

The application upgrade process begins. (Go to the next step.)

- If the release to which you want to upgrade is not listed on the Upgrade Platform page, click **Upload via HTTP** or **Upload via SCP** to upload the necessary Platform image to the Junos Space server.

To upload the new Platform image, perform one of the following steps:

- a. Click **Upload via HTTP**.

The Software File dialog box appears.

- i. Type the name of the file (Junos Space Network Management Platform image) or click **Browse** to navigate to where the new Junos Space Network Management Platform image file is located on the local file system.

- ii. Click **Upload**.

- b. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. You must add the following Secure Copy remote machine credentials.

- i. Add your username.
- ii. Add your password.
- iii. Conform by adding your password again.
- iv. Add the host IP address.

- v. Add the local path name of the Junos Software application file.
- vi. Click **Upload**.

The new Junos Space Network Management Platform image file is uploaded from the local file system into the Junos Space server and is displayed by application name, filename, version, release type, and required Junos Space Network Management Platform version.

When the upload is completed the Upgrade Platform Job Information dialog box appears.

- a. In the Upgrade Application Job Information dialog box, if you click the Job ID link, you see the Upgrade Application job on the **Jobs > Job Management** inventory page.
 - i. Ensure that the job is successful.
 - ii. Select **Administration > Applications** to continue with the add application process.

The Applications inventory page appears.

- b. Select the **Network Management Platform** application and select **Upgrade Platform** from the Actions menu.

The Upgrade Platform dialog box appears. You see the application file that was uploaded.

- c. Select the release image file to which you want to upgrade, and click **Upgrade**.
5. An upgrade warning message appears informing you about the list of applications that might be disabled after the upgrade. Make a note of these applications and upgrade them after the Junos Space Network Management Platform upgrade is completed successfully. Click **OK**.



NOTE: If you are upgrading from Junos Space Network Management Platform Release 13.1 to a later version, say 13.2, another upgrade warning message appears asking you whether you want the system to back up the database before the platform upgrade. Click YES or NO depending on whether you want the system to back up the Junos Space Network Management Platform database before the upgrade.

Backing up the database before the upgrade helps you to recover the data if the platform upgrade fails. However, the upgrade process might be prolonged depending on the database size.

When you choose to back up the database before the upgrade, you are directed to the “Database Backup and Restore” workspace. Follow the instructions specified in [“Backing Up the Junos Space Network Management Platform Database”](#) on page 605 to back up the database.

After backing up the database, select **Administration > Applications > Network Management Platform > Upgrade Platform > Upgrade** action to upgrade Junos Space Network Management Platform. When prompted for the second time, whether you want the system to back up the database, click **NO** to proceed with the upgrade.

6. You enter **Maintenance** mode. Junos Space Network Management Platform prompts you to enter a user name and password to enter maintenance mode. The user name is **maintenance**; the password is one that the administrator created during the initial installation process.
7. Enter the maintenance mode user name and password in the text field.
8. Click **Log In**.

The Junos Space Network Management Platform upgrade process begins. The Software Install Status dialog box appears, which displays status messages using which you can monitor the current upgrade status.

This process might take a while. Wait until the **Return to Maintenance Menu** link appears.

9. Click the **Return to Maintenance Menu** link.

The Maintenance Mode Actions dialog box appears.

10. Click the **Log Out and Exit from Maintenance Mode** link.

The installation progress dialog box appears, which displays the deployment status of JBoss and various other applications as the system goes through a restart after the upgrade. For example, this dialog box displays information about the applications that are being deployed, the timestamp of the deployments, and whether the applications are disabled after the deployment.



CAUTION: This process might take a while. Do not reboot the system for a quick recovery. This action leaves the system in a bad state and affects

the upgrade operation. Wait until the login window is presented for you to log in.

When the installation is complete, the Junos Space login prompt appears.



NOTE: If a blank page appears instead of the login prompt, click Refresh. The login prompt is then displayed.



NOTE: We recommend that you clear the Web browser cache before logging in to the upgraded software.



NOTE: We recommend that you perform a functional audit on all deployed services after upgrading.

You can now log in to begin using the upgraded Junos Space Network Management Platform software.

For any troubleshooting, see the following logs:

- `/var/log/install.log`—This file captures information about the Junos Space Network Management Platform upgrade and the installation of applications.
- `/var/log/jboss/server.log`—This file captures information about JBoss.

Related Documentation

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)
- [Modifying Junos Space Application Settings on page 624](#)
- [Uninstalling a Junos Space Application on page 646](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)

Uninstalling a Junos Space Application

The Uninstall application action allows the administrator to remove a Junos Space application independently while the system is still running. Uninstalling an application cleans up all database data and any process the application used. Uninstall a Junos Space application from the Applications inventory page.

To uninstall a Junos Space application:

1. Select **Administration > Applications**.

The Applications inventory page appears.

2. Select the application you want to uninstall and select **Uninstall Application** from the Actions menu.

The Uninstall Application dialog box appears.

3. Select the application to confirm that you want to uninstall.
4. Click **Uninstall**.

The application uninstall process begins and the Junos Space application is removed from Junos Space Network Management Platform.

The uninstallation might fail if there are any dependent applications. For example, if you try to uninstall Network Activate without uninstalling dependent applications, such as Transport Activate or OAM Insight, the following error message is thrown and the uninstallation fails:

Network Activate Uninstall failed!

Details: Uninstalling Network Activate is not possible until the dependency apps are uninstalled first Transport Activate, OAM Insight, Sync Design & NWappsAPI

Typically, such messages are displayed for applications that are supported from Junos Space Network Management Platform Release 13.1. However, it is also dependent on the type and version of the application being uninstalled.



NOTE: It is important that you uninstall the applications in the right order: from the dependent applications to the primary application.

Related Documentation

- [Application Management Overview on page 621](#)
- [Managing Junos Space Applications on page 622](#)
- [Modifying Junos Space Application Settings on page 624](#)
- [Upgrading a Junos Space Application on page 638](#)
- [Upgrading Junos Space Network Management Platform on page 641](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)

CHAPTER 65

Troubleshoot Space

- [System Status Log File Overview on page 647](#)
- [Customizing Node System Status Log Checking on page 649](#)
- [Customizing Node Log Files To Download on page 650](#)
- [Downloading the Troubleshooting Log File from the UI on page 650](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 652](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 653](#)

System Status Log File Overview

The system writes a system log file for each fabric node to provide troubleshooting and monitoring information. See [“System Status Log File” on page 647](#).

The system administrator can customize the information that is collected in the system log file. See [“Customizing Node System Status Log Checking” on page 649](#).

The system administrator can download the latest log files for each fabric node when logged into a Junos Space Appliance. See [“Downloading System Log Files for a Junos Space Appliance” on page 648](#).

In each operating mode, the system administrator can customize the default log files that are downloaded from a Junos Space Appliance. See [“Customizing Node Log Files To Download” on page 650](#).

System Status Log File

Approximately once a minute, the system checks and writes a status log file **SystemStatusLog** for each fabric node by default. Each log file consists of system status, such as the disk, CPU, and memory usage information, as shown. Junos Space Network Management Platform writes each system status log file to **/var/log/SystemStatusLog**.

```
2009-08-10 11:51:48,673 DEBUG [net.juniper.jmp.cmp.nma.NMAResponse] (Thread-110:)  
Node IP: 192.0.2.0 Filesystem      1K-blocks  Used Available Use% Mounted on  
/dev/mapper/VolGroup00-LogVol00  
       79162184 15234764 59841252 21% /  
Cpu(s): 8.7%us, 1.1%sy, 0.0%ni, 90.0%id, 0.1%wa, 0.0%hi, 0.0%si, 0.0%st  
Mem: 3866536k total, 2624680k used, 1241856k free, 35368k buffers  
Swap: 2031608k total, 941312k used, 1090296k free, 439704k cached
```

Customizing Status Log File Content

The system administrator can customize the information that is written in a fabric node system status log file. For more information, see [“Customizing Node System Status Log Checking” on page 649](#).

Downloading System Log Files for a Junos Space Appliance

The system administrator can download the latest log files for each fabric node when logged into a Junos Space Appliance. The system status log file and all other third party log files are collected and compressed in a troubleshooting file.

[Table 97 on page 648](#) lists the files included in the **troubleshoot** file.

Table 97: Log Files included in the troubleshoot File

Description	Location
System status log file	<code>/var/logSystemStatusLog</code>
Jboss log files	<code>/var/log/jboss/*</code>
Service Provisioning data files	<code>/var/tmp/jboss/debug/*</code>
MYSQL error log	<code>/var/log/mysqld.log</code>
Log files for Apache, NMA, Webproxy	<code>/var/log/httpd/*</code>
Watchdog log file	<code>/var/log/watchdog/*</code>
Linux system messages	<code>/var/log/messages/*</code>

The system administrator can download log files in each operation mode as follow:

- Server Mode (See [“Downloading the Troubleshooting Log File from the UI” on page 650](#).)
- Maintenance Mode (See [“Downloading the Troubleshooting Log File In Maintenance Mode” on page 652](#).)
- CLI mode (See [“Downloading Troubleshooting System Log Files Through the CLI” on page 653](#).)

Customizing Log Files To Download

The system administrator can also customize the log files to be downloaded for specific fabric nodes. For more information, see [“Customizing Node Log Files To Download” on page 650](#).

Related Documentation

- [Maintenance Mode Overview on page 548](#)
- [Customizing Node System Status Log Checking on page 649](#)
- [Customizing Node Log Files To Download on page 650](#)

- [Downloading the Troubleshooting Log File from the UI on page 650](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 652](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 653](#)

Customizing Node System Status Log Checking

The system administrator can customize the system checking for a fabric node so that the necessary information is written to `/var/log/SystemStatusLog`. The administrator must modify the fabric node Perl script in `/usr/nma/bin/writeLogCronJob`.

To customize system status checking for a Junos Space Appliance, modify the `writeSystemStatusLogFile` sub-function in `writeLogCronJob` as shown:

```
sub writeSystemStatusLogFile{
    my $err = 0;
    my $logfile = $_[0];
    $err = system("date >> $logfile");
    $err = system("df /var >> $logfile");
    $err = system("top -n 1 -b | grep Cpu >> $logfile");
    $err = system("top -n 1 -b | grep Mem: >> $logfile");
    $err = system("top -n 1 -b | grep Swap: >> $logfile");

    ***<Add additional system command here that you want to print out in the
    SystemStatusLog file>***

    if ($err == 0 ) {          print "write log to $logfile successfully\n";
    } else {                   print "cannot write log to $logfile\n";
    }
    return $err;
}
```

Related Documentation

- [Maintenance Mode Overview on page 548](#)
- [System Status Log File Overview on page 647](#)
- [Customizing Node Log Files To Download on page 650](#)
- [Downloading the Troubleshooting Log File from the UI on page 650](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 652](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 653](#)

Customizing Node Log Files To Download

The system administrator can customize the log files that are downloaded for each fabric node by modifying the Perl script in `/var/www/cgi-bin/getLogFiles`.

To customize the log files that are downloaded for each fabric node, modify the `getLogFiles` Perl script zip command as shown:

```
...
system("zip -r $logFileName /var/log/jboss/* /var/tmp/jboss/debug/
/var/log/mysqld.log /var/log/httpd/* /var/log/watchdog /var/log/messages
/var/log/SystemStatusLog > /dev/null");
...
```

Related Documentation

- [Maintenance Mode Overview on page 548](#)
- [System Status Log File Overview on page 647](#)
- [Customizing Node System Status Log Checking on page 649](#)
- [Downloading the Troubleshooting Log File from the UI on page 650](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 652](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 653](#)

Downloading the Troubleshooting Log File from the UI

From the Administration workspace, the system administrator can download a troubleshooting file `troubleshoot_yyyy-mm-dd_hh-mm-ss.zip` that contains useful information for managing and monitoring the nodes in the system. The troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, `troubleshoot_2010-04-01_11-25-12.zip`.

To retrieve troubleshooting data and log files, follow these steps:

1. Select **Administration > Troubleshoot space**.

The Troubleshoot SPACE page appears.

2. Click the **Download troubleshooting data and logs from SPACE** link to access the `troubleshoot_yyyy-mm-dd_hh-mm-ss.zip` file in your browser.

- If you are using Mozilla Firefox: In the Opening troubleshoot zip dialog box, select **Save file** and click **OK** to save the zip file to your computer using the Firefox Downloads dialog box.
- If you are using Internet Explorer: From the File Download screen, select **Save** and select a directory on your computer where you want to save the `troubleshoot_yyyy-mm-dd_hh-mm-ss.zip` file.

3. When you contact the Juniper Technical Assistance Center, describe the problem you encountered and provide the JTAC representative with the `troubleshoot.zip` file.

Table 98 on page 651 lists the files included in the `troubleshoot_YYYY-MM-DD_HH-MM-SS.zip` file.

Table 98: Data and Log Files in troubleshoot.zip File

Description	Location
Jboss log files	<code>/var/log/jboss/*</code>
Service Provisioning data files	<code>/var/tmp/jboss/debug/*</code>
MYSQL error log	<code>/var/log/mysqld.log</code>
Log files for Apache, NMA, Webproxy	<code>/var/log/httpd/*</code>
Watchdog log file	<code>/var/log/watchdog/*</code>
Linux system messages	<code>/var/log/messages/*</code>
CPU/RAM/Disk statistics (during past 24 hours)	Not applicable

Related Documentation

- [Maintenance Mode Overview on page 548](#)
- [System Status Log File Overview on page 647](#)
- [Customizing Node System Status Log Checking on page 649](#)
- [Customizing Node Log Files To Download on page 650](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 652](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 653](#)

Downloading the Troubleshooting Log File In Maintenance Mode

Maintenance Mode is a special mode that an administrator can use to perform system recovery or debugging tasks while all nodes in the fabric are shutdown and the web proxy is running.

The administrator can download the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file from Maintenance Mode. The troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

To download the troubleshooting log file in maintenance mode, follow these steps:

1. Connect to a Junos Space Appliance in maintenance mode by using the Junos Space Appliance URL.

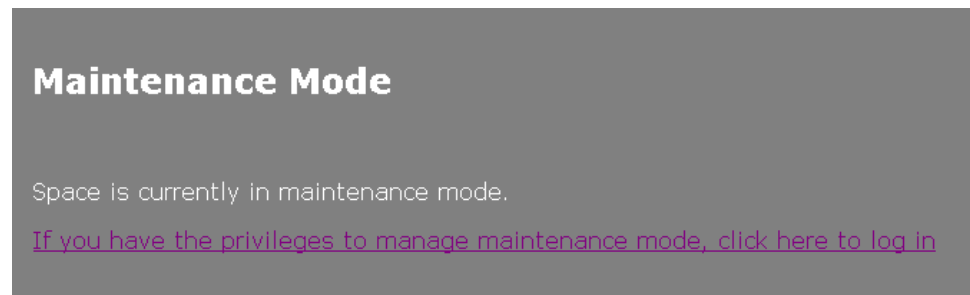
For example:

`https://<ipaddress>/maintenance`

Where *ipaddress* is the address of the Junos Space Appliance.

The Maintenance Mode page appears.

Figure 79: Maintenance Mode Page



2. Click the **click here to log in** link. The login dialog box appears.
3. Log in to maintenance mode using the authorized login name and password.
4. Click OK. The Maintenance Mode Actions menu appears.
5. Click **Download Troubleshooting Data and Logs**. The file download dialog box appears.
6. Click Save to download the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file to the connected computer.
7. Click **Log Out and Exit from Maintenance Mode**.

Related Documentation

- [Maintenance Mode Overview on page 548](#)
- [System Status Log File Overview on page 647](#)
- [Customizing Node System Status Log Checking on page 649](#)
- [Customizing Node Log Files To Download on page 650](#)
- [Downloading the Troubleshooting Log File from the UI on page 650](#)

- [Downloading Troubleshooting System Log Files Through the CLI on page 653](#)

Downloading Troubleshooting System Log Files Using the CLI

If Junos Space Network Management Platform is operating, the administrator can log into a Junos Space Appliance console and download system status logs for each fabric node using the CLI Network Settings Utility > SecureCoPy (SCP) command. If the system is not operating, the Administrator can download system status logs using the CLI USB command.

The Network Settings Utility, for both commands, collects all system log files in the `/var/log` subdirectory and creates a `*TAR` file to download. For more information on the log files that are written, see “[System Status Log File Overview](#)” on page 647.

This procedure includes the following tasks:

- [Downloading a System Log File Using a USB Device on page 653](#)
- [Downloading System Log File Using SCP on page 654](#)

Downloading a System Log File Using a USB Device

Using the Networks Settings Utility Retrieve Logs > USB command, the administrator can download system status logs to a connected USB device if the network is down.

1. Using a console utility, such as SSH or Telnet, connect to the Junos Space Appliance. The Junos Space Settings Menu appears.

Junos Space Settings Menu

```
1> Change Password
2> Set Routing
3> Set DNS Servers
4> Change Time Options
5> Retrieve Logs
6> Security
7> (Debug) run shell
```

```
Q> Quit
R> Redraw Menu
```

Choice [1-7,QR]:

2. Type option **5> Retrieve Logs**. The Retrieve Logs submenu appears.

Choice [1-7,QR]: 5

```
1> Save to USB
2> Send via SCP
```

```
M> Return to Main Menu
R> Redraw Menu
```

Choice [1-2,MR]:

3. Select **1> Save to USB**. The USB device must be connected to a Junos Space Appliance.
4. Indicate whether you want to continue. Enter **y** for yes; **n** to abort.
5. The Save to USB process downloads the log files from all cluster members and combines them into a **.tar** file. Once the file is created, the process copies the file onto a USB device. You see the following:

Copying 20090827-1511-logs.tar to USB drive

Downloading System Log File Using SCP

Using the Networks Settings Utility Retrieve Logs > SCP command, the administrator can download system status logs to a specific location.

To download system status logs using SCP, follow these steps:

1. Using a console utility, such as SSH or Telnet, connect to a Junos Space Appliance. The Junos Space Settings Menu appears.

Junos Space Settings Menu

1> Change Password
2> Set Routing
3> Set DNS Servers
4> Change Time Options
5> Retrieve Logs
6> Security
7> (Debug) run shell

Q> Quit
R> Redraw Menu

Choice [1-7,QR]:

2. Type option **5> Retrieve Logs**. The Retrieve Logs submenu appears.

Choice [1-7,QR]: 5

1> Save to USB
2> Send via SCP

M> Return to Main Menu
R> Redraw Menu

Choice [1-2,MR]:

3. Select **2> Send via SCP**. The process retrieves the log files on all cluster members and combines them into a **.TAR** file.
4. Indicate whether you want to continue. Enter **y** for yes; **n** to abort.
5. Specify the SCP server IP address to which to transfer the file.
6. Enter the remote SCP user. For example, **root**
7. Enter the remote SCP file location. For example, **/root/tmplogs**. You see the following:

```

Remote scp IP: 192.0.2.0
Remote scp user: root
Remote scp path: /root/tmplogs
Is this correct? [y/n]
The authenticity of host '192.0.2.0 (192.0.2.0)' can't be established.
RSA key fingerprint is 01:70:4c:47:9e:1e:84:fc:69:3c:65:99:6d:e6:88:87.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.0.2.0' (RSA) to the list of known hosts.
Warning-Please dont use this system
/etc/selinux/strict/contexts/files/file_contexts: Multiple same specifications for
/usr/local/lost\+found/*
/etc/selinux/strict/contexts/files/file_contexts: Multiple same specifications for
/usr/local/\.journal
/etc/selinux/strict/contexts/files/file_contexts: Multiple same specifications for
/usr/local/lost\+found.
192.0.2.0 password:
20090827-1517-logs.tar
100% 18MB 17.6MB/s 00:01

```

8. Indicate whether the SCP server information is correct. Enter **y** for yes; **n** if incorrect.
9. Indicate whether you want to continue. Enter **y** for yes; **n** for no.

**Related
Documentation**

- [Maintenance Mode Overview on page 548](#)
- [System Status Log File Overview on page 647](#)
- [Customizing Node System Status Log Checking on page 649](#)
- [Customizing Node Log Files To Download on page 650](#)
- [Downloading the Troubleshooting Log File from the UI on page 650](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 652](#)

CHAPTER 66

Manage Certificates

- [Certificate Management Overview on page 657](#)
- [Installing Custom SSL Certificate on the Junos Space Server on page 662](#)

Certificate Management Overview

Typically, users gain access to resources from an application or system on the basis of their username and password. You can also use certificates to authenticate and authorize sessions among various servers and users. Certificate-based authentication over an SSL connection is the most secure type of authentication. The certificates can be stored on a smart card, a USB token, or a computer's hard drive. The users typically swipe their smart card to log in to the system without entering their username and password.

See the following sections to upload the certificates to the Junos Space server and to enable certificate-based authentication:

- [Workflow on page 657](#)
- [Loading a Custom Junos Space Server Certificate on page 659](#)
- [Loading a User Certificate on page 659](#)
- [Loading CA Certificates and CRLs on page 660](#)
- [Changing the Authentication Mode on page 661](#)
- [Invalid Certificates on page 662](#)

Workflow

The basic steps in establishing an SSL connection for the different modes of authentication are as follows:

- Certificate-based authentication:
 - A client requests access to the Junos Space server.
 - The Junos Space server presents its certificate to the client.
 - The client verifies the server's certificate.
 - If the verification of the certificate is successful, then the client sends its certificate to the server.

- The server verifies the credentials of the client.
- If the verification is successful, then the server grants access to the protected resource requested by the client. If the user is not found, Junos Space Network Management Platform sends a login failure page to the user and the current SSL session is terminated.

The session is also terminated when the smart or secure card (containing the certificate and the private key) that is used for logging in is unplugged or removed from the client system.

- Username and password-based authentication:
 - A client requests access to the Junos Space server.
 - The Junos Space server presents its certificate to the client.
 - The client verifies the server's certificate.
 - If the verification of the certificate is successful, then the client sends its username and password to the server.
 - The server verifies the credentials of the client.
 - If the verification is successful, then the server grants access to the protected resource requested by the client.

Junos Space Network Management Platform ships with the default password-based authentication mode. Administrators can use the default credentials to log in to Junos Space Network Management Platform.

From Junos Space Network Management Platform Release 13.1 onward, Junos Space Network Management Platform supports both certificate-based authentication as well password-based authentication. However, only one authentication mode is supported at a time and all the users are authenticated using the designated authentication mode.

Before you change the authentication mode from password-based to certificate-based, upload the CA certificates and the personal or user certificates (Junos Space server certificate is optional) to the Junos Space server. Junos Space Network Management Platform verifies all the certificates when they are uploaded. Invalid or badly formed certificates are not uploaded.

You need not restart Junos Space Network Management Platform when you switch from one authentication mode to another. However, when the authentication mode is changed, all the existing user sessions, except that of the current administrator who is changing the authentication mode, are automatically terminated and the users are forced to log out.

The basic workflow to enable certificate-based authentication mode is as follows:

1. (Optional) Load the server certificate to the Junos Space server (from Administration > Platform Certificate).

If you do not upload a customized server certificate, then the default Junos Space Network Management Platform certificate is used.

See [“Loading a Custom Junos Space Server Certificate” on page 659](#).

2. Load the user certificate:

- For a new local user (from User > User Accounts > Create User).

See [“Loading a User Certificate” on page 659](#).

- For existing local users (from User > User Accounts > Modify User or User Preferences).

See [“Loading a User Certificate” on page 659](#).

3. Load the CA certificates and the certificate revocation list (from Administration > CA/CRL Certificates).

See [“Loading CA Certificates and CRLs” on page 660](#).

4. Enable certificate-based authentication mode (from Administration > Applications > Network Management Platform > Modify Application Settings > User > Use X509 Certificate Auth Mode).

See [“Changing the Authentication Mode” on page 661](#).

Loading a Custom Junos Space Server Certificate

By default, the Junos Space Network Management Platform uses a self-signed SSL certificate provided by Juniper Networks. However, if there is a need to use your own custom certificate, Junos Space Network Management Platform provides an option to upload your custom certificate from Administration > Platform Certificate, as an X.509 certificate or PKCS #12 certificate. For instructions to upload your custom certificate, see [“Installing Custom SSL Certificate on the Junos Space Server” on page 662](#).

Loading a User Certificate

If you are opting for a certificate-based authentication mode, then for each user you need to upload the corresponding certificate for the Junos Space server to authenticate the user. You can associate a certificate with a user at the time of creation of the user or by modifying the user settings from the Modify User page (for an existing user).

Before you proceed, make sure that the user certificate is available on your local system.

- To upload a certificate for a new user:
 1. Select **Network Management Platform > Users > User Accounts > Create User**. The Create User page appears.
 2. Enter values for the mandatory fields, such as “Login ID.” For detailed information about the fields that appear on this page, see [“Creating User Accounts” on page 509](#).

3. Click **Browse** adjacent to the **X509 Cert File** field to navigate to the location of the X.509 certificate file on your local system.
 4. Click **Upload**.
 5. Click **Finish**.
- To upload a certificate for an existing user:

The following instructions are for an existing user who is currently logged in:

1. Click **User Preferences**. The Change Local Password and Certificate dialog box appears.
2. Click **Browse** adjacent to the **X509 Cert File** field to navigate to the location of the X.509 certificate file on your local system.
3. Click **Upload**.
4. Click **OK**.

To modify an existing user other than the user who is currently logged in:

1. Select **Network Management Platform > Users > User Accounts > Modify User**. The Modify User page appears.
2. Click **Browse** adjacent to the **X509 Cert File** field to navigate to the location of the X.509 certificate file on your local system.
3. Click **Upload**.
4. Click **Finish**.

Loading CA Certificates and CRLs

A CA certificate or the root certificate is used to verify a user certificate. The private key of the root certificate is used to sign the user certificates, which then inherit the trustworthiness of the root certificate.

A certificate revocation list (CRL), which is maintained by a CA, is a list of certificates that were issued and revoked by that CA before their scheduled expiration date, along with the reasons for revocation. A Certificate Authority (CA) may revoke a certificate for various reasons, such as the user specified in the certificate may no longer have the authority to use the key, the key specified in the certificate might have been compromised, another certificate is replacing the current certificate, and so on.

Before you proceed, make sure that the CA certificate or the CRL is available on your local system.

To upload a CA certificate:

1. Select **Administration > CA/CRL Certificates**.

The CA/CRL Certificates page appears. This page displays the previously uploaded CA certificates.

2. Click the arrow mark next to the **+** icon and select **X.509 CA Certificate** icon.

The Upload X.509 CA Certificate page appears.

3. Click **Browse** adjacent to the **X.509 CA Certificate File** field to navigate to the location of the X.509 certificate file on your local system.

4. Click **Upload**.

To upload a CRL certificate:

1. Select **Administration > CA/CRL Certificates**.

The CA/CRL Certificates page appears. This page displays the previously uploaded CRLs.

2. Click the arrow mark next to the **+** icon and select **X.509 CRL Certificate** icon.

The Upload X.509 CRL Certificate page appears.

3. Click **Browse** adjacent to the **X.509 CRL Certificate File** field to navigate to the location of the X.509 CRL file on your local system.

4. Click **Upload**.

To delete any CA certificates or CRLs, select them and click the **Delete X509 CA/CRL Certificate** icon. Click **Yes** on the confirmation page.

Changing the Authentication Mode

After uploading the certificates for the Junos Space server and users, you can change the authentication mode from the default password-based authentication to certificate-based authentication:

1. Select **Applications > Network Management Platform > Modify Application Settings > User**. The Modify Network Management Platform Settings page appears.
2. Select **Use X509 Certificate Auth Mode**.
3. Click **Modify**.



CAUTION: When the authentication mode is changed, all the existing user sessions are automatically terminated and users are forced to log out except for the current administrator who is changing the authentication mode.

If the certificate is scheduled to expire within 30 days from the current date, a warning message appears at the time of logging in to indicate that the certificate will expire after these many days. Reload your certificate from the User Preferences page or request the administrator to reload it from the Modify User page. If a user tries to log in with an invalid certificate, Junos Space Network Management Platform displays a login failure page with the **No user mapped for this certificate** message. You could face this issue when the certificate is expired. If you have a valid username and password, switch to password-based authentication mode from the Junos Space server system console and try logging in.

To change the authentication mode from the system console:

1. Log on to the Junos Space server system console (that is running as the VIP node) as the root user.
2. Navigate to the following directory: **/var/www/cgi-bin**.
3. Type the following command:
setSpaceAuthMode password-based

This command sets the authentication mode to password-based for all the users. When the authentication mode is changed, all the existing user sessions are automatically terminated and users are forced to log out except for the current administrator who is changing the authentication mode.

Invalid Certificates

A certificate could become invalid for the following reasons:

- Certificate is expired.
- Certificate expires within a day.
- Certificate will be valid only later.
- Certificate does not match the private key.
- Certificate or private key file is broken.
- Same certificate exists in Junos Space.

Related Documentation

- [Installing Custom SSL Certificate on the Junos Space Server on page 662](#)

Installing Custom SSL Certificate on the Junos Space Server

The topics in this section describe how to associate your own custom SSL certificate with the Junos Space server.

- [Changing the Default Junos Space Server SSL Certificate on page 663](#)
- [Installing an X.509 Junos Space Server Certificate on page 663](#)
- [Installing a PKCS #12 Format Junos Space Server Certificate on page 664](#)

- [Certificate Expiry on page 665](#)
- [Certificate Attributes on page 665](#)

Changing the Default Junos Space Server SSL Certificate

Junos Space Network Management Platform uses the default SSL certificate signed by Juniper Networks. However, Junos Space Network Management Platform provides an option to associate your own custom SSL certificate with the Junos Space server.

To install your custom certificate:

1. Select **Network Management Platform > Administration > Platform Certificate**. The Platform Certificate page appears.

You can upload a certificate in X.509 format or PKCS # 12 format.

The upper portion of the page displays the certificate that is currently being used by the Junos Space server. By default, Junos Space Network Management Platform uses the SSL certificate signed by Juniper Networks. To gain an understanding about the attributes of the certificate, see [Table 99 on page 665](#).

2. To install an X.509 certificate, see [“Installing an X.509 Junos Space Server Certificate” on page 663](#).

To install a PKCS #12 format certificate, see [“Installing a PKCS #12 Format Junos Space Server Certificate” on page 664](#).

To revert to the default SSL certificate, click **Use Default Certificate**.

Installing an X.509 Junos Space Server Certificate

X.509 is a widely used standard for defining digital certificates. Typically, in X.509 format, the certificate and the key are stored separately. Because the Junos Space server needs both the certificate and the key, make sure that both the files are available on your local system before you proceed any further. The private key can be either encrypted or unencrypted. Although pass-phrase is optional, it is required if the private key is encrypted.

To install an X.509 certificate file:

1. Select **Network Management Platform > Administration > Platform Certificate**. The Platform Certificate page appears.
2. Select **X.509 Certificate & Private Key** to upload Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (DER) format certificate files. By default, this option is selected.

- DER format certificate files:

- The supported extensions are: .der, .cer, and .crt.
- They are stored in binary format.

- PEM format certificate files:

- The supported extensions are: .pem, .cer, and .crt.
- They are stored in Base64-encoded DER format.

3. To navigate to the X.509 certificate file on your local file system, click **Browse** adjacent to the **Certificate** field.
4. To navigate to the private key file on your local file system, click **Browse** adjacent to the **Private Key** field.
5. (Optional) Enter the pass-phrase in the **Private Key Pass-phrase** field. Make sure that you enter the pass-phrase if the private key is encrypted.
6. Click **Upload**.

Junos Space Network Management Platform displays a warning message asking for confirmation whether the current certificate can be replaced. If you click **Cancel**, Junos Space Network Management Platform continues to use the current certificate. If you click **Yes**, then Junos Space Network Management Platform performs internal validations to verify whether the uploaded files are valid. If the files are valid, then the upload is successful and Junos Space Network Management Platform starts using the new certificate. All the existing sessions are terminated and the users are forced to log out. However, if the files are invalid, Junos Space Network Management Platform throws an error.

Installing a PKCS #12 Format Junos Space Server Certificate

The Personal Information Exchange Syntax Standard (PKCS) #12 format is a widely used format for digital certificates in the Windows operating system. This standard specifies a portable format for storing or transporting a user's private keys, certificates, and pass-phrases in one encryptable file. After you upload this file, Junos Space Network Management Platform converts it into two files (public certificate and decrypted private key) in PEM format.

Before you proceed, make sure that the PKCS #12 certificate is available on your local file system.

1. Select **Network Management Platform > Administration > Platform Certificate**. The Platform Certificate page appears.
2. Select **PKCS #12 Format Certificate** to upload PKCS#12 format certificate files.
3. Click **Browse** adjacent to the **Certificate & Private Key** field to navigate to the PKCS#12 format certificate file on your local file system.
4. (Optional) Enter the password in the **Password** field.
5. Click **Upload**.

Junos Space Network Management Platform displays a warning message asking for confirmation whether the current certificate can be replaced. If you click **Cancel**, Junos Space Network Management Platform continues to use the current certificate. If you click **Yes**, then Junos Space Network Management Platform performs internal validations to verify whether the uploaded file is valid. If the file is valid, then the upload is successful and Junos Space Network Management Platform starts using the new certificate. All the existing sessions are terminated and the users are forced to log out. However, if the file is invalid, Junos Space Network Management Platform throws an error.

Certificate Expiry

When the Junos Space server certificate is scheduled to expire within 30 days from the current date, Junos Space Network Management Platform throws a warning message every time the administrator logs in. For example:

Your platform certificate is going to expire on May 24, 2013. Space will automatically use default certificate if your certificate will expire within 1 day. Change platform certificate using "Administration > Platform Certificate" page. Would you like to change it now?

When the Junos Space server certificate is scheduled to expire in a day, Junos Space Network Management Platform starts using the default certificate.

As an administrator, perform one of the following actions:

- Upload a new certificate. Junos Space Network Management Platform deletes the old user certificate and starts using the newly uploaded certificate.
- Use the default certificate—Click **Administration > Platform Certificate > Use Default Certificate**.

Certificate Attributes

Table 99 on page 665 lists the attributes that you commonly see in a certificate.

Table 99: Certificate Attributes

Certificate Attribute	Description
Subject Name: OID.1.2.840.113549.1.9.1=root@10.205.57.195	"OID.1.2.840.113549.1.9.1" is the ASN.1 object identifier used to identify this signature algorithm. "root@10.205.57.195" is the e-mail address of the certificate owner.
Subject Name: CN	Common name of the certificate owner
Subject Name: OU	Name of the organizational unit to which the certificate owner belongs. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " Junos Space " for this attribute.
Subject Name: O	Organization to which the certificate owner belongs. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " Juniper Networks, Inc. " for this attribute.
Subject Name: L	Certificate owner's location. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " Sunnyvale " for this attribute.
Subject Name: ST	Certificate owner's state of residence. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " California " for this attribute.

Table 99: Certificate Attributes (*continued*)

Certificate Attribute	Description
Subject Name: C	Certificate owner's country of residence. For example, "US."
Issuer Name: OID.1.2.840.113549.1.9.1=root@10.205.57.195	"OID.1.2.840.113549.1.9.1" is the ASN.1 object identifier used to identify this signature algorithm. "root@10.205.57.195" is the e-mail address of issuer.
Issuer Name: CN	Common name of the certificate issuer. It is the IP address of the system. The common name (CN) must match the hostname of the issuer of this certificate. In general, it should be the hostname of issuer.
Issuer Name: OU	Name of the organizational unit to which the certificate issuer belongs For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " Junos Space " for this attribute.
Issuer Name: O	Organization to which the certificate issuer belongs. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " Juniper Networks, Inc. " for this attribute.
Issuer Name: L	Certificate issuer's location. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " Sunnyvale " for this attribute.
Issuer Name: ST	Certificate issuer's state of residence. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains " California " for this attribute.
Issuer Name: C	Certificate issuer's country of residence. For example, "US."
Signature Algorithm Name	Algorithm used by the Certificate Authority to sign the certificate. For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks can contain " SHA1withRSA " for this attribute.
Serial Number	Certificate's serial number
Not Before	Date at which the certificate becomes valid
Not After	Date at which the certificate becomes invalid

Related Documentation • [Certificate Management Overview on page 657](#)

CHAPTER 67

Manage Authentication Servers

- [Remote Authentication Overview on page 667](#)
- [Understanding Junos Space Authentication Modes on page 668](#)
- [Managing Remote Authentication Servers on page 669](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 673](#)
- [Configuring TACACS+ for Authentication and Authorization on page 677](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Remote Authentication Overview

Junos Space Network Management Platform, by default, authenticates users to log in locally when you configure their accounts using **Users > User Accounts > Create User** task.

Using the **Administration > Authentication Servers** task, you can authenticate users to log in exclusively from a centralized location using one or more RADIUS remote authentication servers. You can also authenticate users to log in to Junos Space Network Management Platform using both local and remote authentication.

You can configure the order in which Junos Space Network Management Platform connects to remote authentication servers by preference. Junos Space Network Management Platform authenticates using the first reachable remote authentication server on the list.

You must install or upgrade to Junos Space Release 11.2 or later to use remote authentication, and to Junos Space Release 12.1 or later to use remote authorization.

Junos Space Network Management Platform supports RADIUS authentication methods PAP and CHAP.

You must have Super Administrator, System Administrator privileges to configure remote authentication server settings, authentication modes, and user passwords and settings.

Regular Junos Space Network Management Platform users cannot configure their own passwords if you maintain them solely by a remote authentication server.

You may choose to allow some privileged users to set a local password so they can still log onto the system if the remote authentication server is unreachable.

**Related
Documentation**

- [Junos Space Authentication Modes Overview on page 668](#)
- [Managing Remote Authentication Servers on page 669](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Understanding Junos Space Authentication Modes

Junos Space Network Management Platform provides three authentication modes: local, remote, and remote-local. The default authentication mode is local. You configure local authentication from **Users > User Accounts > Create Users** task. You configure remote and remote-local authentication from **Administration > Remote Auth Servers** task.



NOTE: You configure local authorization from **Users > Roles > Create Roles** task. See [“Configuring Users to Manage Objects in Junos Space Overview” on page 480](#), [“Creating User Accounts” on page 509](#), and [“Creating a User-Defined Role” on page 505](#).

The following sections describe the authentication modes:

- [Local Authentication on page 668](#)
- [Remote Authentication on page 668](#)
- [Remote-Local Authentication on page 669](#)

Local Authentication

The user is authenticated and authorized using the local Junos Space Network Management Platform database. To configure local Junos Space Network Management Platform authentication, navigate to **> Users > User Accounts > Create Users** icon. To configure Junos Space Network Management Platform authentication, see [“Creating User Accounts” on page 509](#).

Remote Authentication

User authentication information is stored on one or more remote authorization servers. Authorization information also can be configured and stored on the remote authentication server(s). To configure Junos Space Network Management Platform remote authentication, see [“Configuring a RADIUS Server for Authentication and Authorization” on page 673](#).

In this mode, if a corresponding local user exists, the local password is used only in the emergency case where the authentication servers are unreachable.

Remote-Local Authentication

User authentication information is stored on one or more remote authentication servers. Authorization information also can be configured and stored on the remote authentication server(s). For more information see [“Configuring a RADIUS Server for Authentication and Authorization” on page 673](#).

In this mode, when a user is not configured on the remote authentication server(s) or when the server(s) are unreachable or when the remote server(s) deny the user access, then the local password is used if such a local user exists in the Junos Space Network Management Platform database.

Related Documentation

- [Remote Authentication Overview on page 667](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 673](#)
- [Configuring TACACS+ for Authentication and Authorization on page 677](#)
- [Managing Remote Authentication Servers on page 669](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)

Managing Remote Authentication Servers

The **Administration > Auth Server** page allows you to configure remote authentication settings to allow users to log in to Junos Space Network Management Platform from a remote authentication server. The **Auth Server** page includes two areas: **Auth Mode Settings** and **Remote Authentication Servers** table.

From the **Auth Mode Settings** area, you can select and save the Junos Space Network Management Platform authentication mode: local, remote, or remote-local.

From the **Remote Authentication Servers** table area, you can:

- Create, modify, and delete remote authentication server connection settings and test the connection.
- Specify the remote authentication server connection order.

To select the remote authentication mode and manage remote authentication servers:

1. Select **Administration > Auth Servers**.
2. In the **Auth Mode Settings** area, select the authentication method you want to use.

By default, Junos Space Network Management Platform is in local authentication mode and the controls for the **Remote Authentication Server** table are disabled. If you select the Use **Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled.

3. Click **Save** to store the remote authentication mode setting you select.

4. In the **Authentication Servers** table Add a new remote authentication server by clicking Add (+). See [“Creating a Remote Authentication Server” on page 670](#).
5. Modify an authentication server by doubling clicking that server row in the table. See [“Modifying Authentication Settings” on page 672](#).
6. Delete an authentication server by selecting that row and clicking Delete (X) to remove an authentication server.
7. Click a row and select the arrows to move the server up and down the list. Up arrow is disabled if at the top of the list; down arrow is disabled if at the bottom of the list.

Sorting for columns are disabled, since there is an explicit sort order as determined by the arrows.
8. On selection of the server, click **Test Connection** to display a transient result of last connection test.
9. Confirm that you want to test the server connection.

After testing, the Status dialog box appears displaying the test results: success or failure.
10. Click OK.

If the connection results fails, ensure the server settings are correct.

Related Documentation

- [Remote Authentication Overview on page 667](#)
- [Junos Space Authentication Modes Overview on page 668](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Creating a Remote Authentication Server

To run Junos Space Network Management Platform remote authentication, you must create one or more remote authentication servers and configure the server settings

To create a remote authentication server:

1. Select **Administration > Auth Servers**.
2. In the Auth Mode Settings area, select the authentication method you want to use.

In local authentication mode, the controls for the Remote Authentication Server table are enabled so you can add authentication servers first and only switch to non-local authentication mode when you are ready later. If you select the Use Remote Authentication check box, you can then select the Remote Authentication Only or the Remote-Local Authentication option.
3. Click **Save** to store the remote authentication mode setting you select.

4. In the Authentication Servers table, add a new remote authentication server by clicking Add (+).

The Create Auth Server dialog box appears.

5. Enter the required settings to connect Junos Space Network Management Platform to the remote authentication server. See [Table 100 on page 671](#).

Table 100: Remote Authentication Server Settings

Setting	Description
Protocol	<p>The supported authentication protocols:</p> <ul style="list-style-type: none"> • PAP—Password Authentication Protocol. This default protocol provides a two-way handshake during the initiation of the connection with the remote authentication server and Junos Space Network Management Platform. PAP requires on a username and password RADIUS attributes. It is protected by the RADIUS shared secret. • CHAP—Challenge Handshake Authentication Protocol. The remote authentication server sends a challenge and the Junos Space Network Management Platform responds with the password and the challenge.
IP Address	The IP address of the remote authentication server. The IPv4 address that you use must be a valid address. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses.
Port Number	The remote authentication server assigned UDP port number. The default is 1812. RADIUS has been officially assigned UDP port 1812 for RADIUS Authentication.
Shared Secret	The text string that serves as a password between the RADIUS server, proxy, and client.
Number of Tries	The number of retries that a device can attempt to contact a RADIUS authentication server. The default tries is 3.
Max Retry Timeout MSecs	The interval in milliseconds Junos Space Network Management Platform waits for a reply from a remote authentication server. The default value is 6000. The retry timeout improves server access on busy networks where overall response times may vary widely from network to network.

6. In the Create Auth Server dialog box, click **OK**.

The remote authentication server appears as a row at the bottom of the table.

7. In the Manage Auth Servers page, click **Test Connection** to verify the Junos Space Network Management Platform connection to the remote authentication server.
 - If the test connection result is a success, the remote authentication server is reachable.
 - If the test connection result is a failure, the remote authentication server is unreachable.

- If the test connection result displays the message *Mismatched shared secret*, then the configured shared secret for that server is incorrect. Ensure that you have entered the correct remote authentication server shared secret details.

**Related
Documentation**

- [Remote Authentication Overview on page 667](#)
- [Junos Space Authentication Modes Overview on page 668](#)
- [Modifying Authentication Settings on page 672](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 673](#)

Modifying Authentication Settings

The Manage Authentication Servers page allows you to change Junos Space Network Management Platform authentication mode and remote authentication server connection settings.

To modify remote authentication settings:

1. In the Mode Settings area, change to the authentication method you want to use.

By default, Junos Space Network Management Platform is in local authentication mode and the controls for the **Remote Authentication Server** table are disabled. If you select the Use **Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled. Mousing over the help icon, displays a description of the available authentication modes.
2. Click **Save** to store the remote authentication mode setting you select.
3. In the Authentication Servers table click the server edit icon that you want to modify. See [“Creating a Remote Authentication Server” on page 670](#).

The Modify Authentication Server dialog box appears.

4. Change the remote authentication server settings you want to change.

For a description of the available remote authentication server, see [“Creating a Remote Authentication Server” on page 670](#).

5. In the Create Auth Server dialog box, click **OK**.

The modified remote authentication server settings are saved in the database.

6. On the Manage Auth Servers page, click **Test Connection** to verify the Junos Space Network Management Platform connection to the remote authentication server.

If the connection is successful, you see **Remote Authentication Server # is reachable**. If the connection is unsuccessful, you see **Remote Authentication Server # is unreachable**. Check to ensure that you have entered the correct remote authentication server settings.

**Related
Documentation**

- [Remote Authentication Overview on page 667](#)
- [Junos Space Authentication Modes Overview on page 668](#)

- [Creating a Remote Authentication Server on page 670](#)
- [Managing Remote Authentication Servers on page 669](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Configuring a RADIUS Server for Authentication and Authorization

Junos Space Network Management Platform supports authorization of users from a RADIUS server. Using the Platform > Administration > Manage Auth Servers workspace, you can configure a RADIUS server to authenticate and authorize users to log in exclusively from a centralized location using one or more RADIUS remote authentication servers. You can also authenticate and authorize users to log in to Junos Space Network Management Platform using both local and remote authentication and authorization.

Authorization data in the RADIUS server are stored as vendor-specific attributes (VSAs). Therefore, you need to update the Junos dictionary file (juniper.dct) in the RADIUS server with the Junos Space Network Management Platform defined VSA (Juniper-Junospace-Profiles). Users in the RADIUS server database should be assigned VSAs, the values of which must correspond to the remote profiles created in the Junos Space server.



NOTE: You must create remote profiles in the Junos Space server before you configure users at the RADIUS server for authorization (see [“Creating a Remote Profile” on page 525](#)).

To configure VSAs (Steel-Belted RADIUS):

1. Add the Junos Space VSA to the Juniper dictionary file (juniper.dct).
`ATTRIBUTE Juniper-Junospace-Profiles Juniper-VSA(11, string) r`
2. Assign a remote profile to the user using the Juniper-Junospace-Profiles attribute.

To configure VSAs (Free RADIUS):

1. Add the Junos Space VSA to the Juniper dictionary file (dictionary.juniper).
`ATTRIBUTE Juniper-Junospace-Profiles 11 String`
2. Assign a remote profile to the user using the VSA. For example:
`"guestuser" Auth-Type:=PAP, User-Password:="<password>"
Juniper-Junospace-Profiles = "guestprofile"`



NOTE: The remote profiles created in Junos Space Network Management Platform are not automatically synchronized to the RADIUS server for selection. The administrator must manually enter the correct remote profile name.

To authenticate and authorize users from the RADIUS server:

1. Select **Administration > Auth Servers**.
2. Under Auth Mode Setting, select the Use Remote Authentication check box.
3. Select either Remote Authentication Only or Remote-Local Authentication.
System behavior differs under these two cases. Some differences occur when a remote RADIUS server rejects authentication of the user. There are also differences in the source of authorization depending on what answer the RADIUS server returns.

If neither Remote Authentication Only nor Remote-Local Authentication is selected, no RADIUS server is used, and the user is authenticated in the Junos Space Network Management Platform database. Authorization is done from the roles present there.

Figure 1 shows the decision tree underlying system behavior when either Remote Authentication Only or Remote-Local Authentication is chosen and a remote RADIUS server accepts the user.

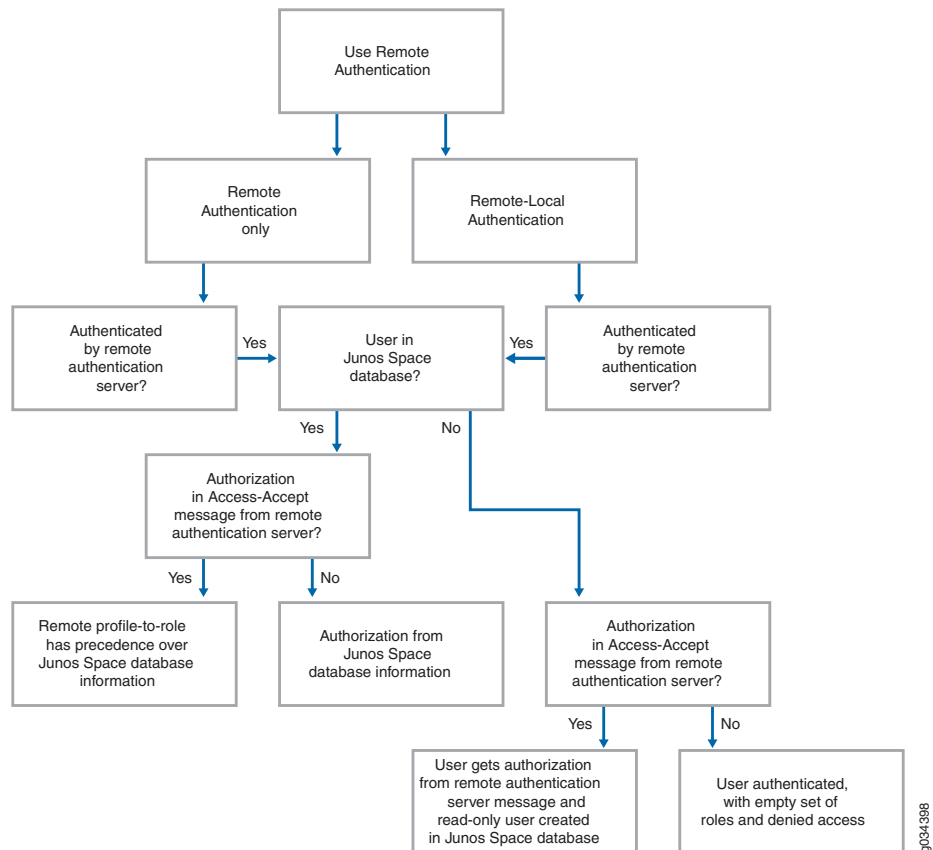
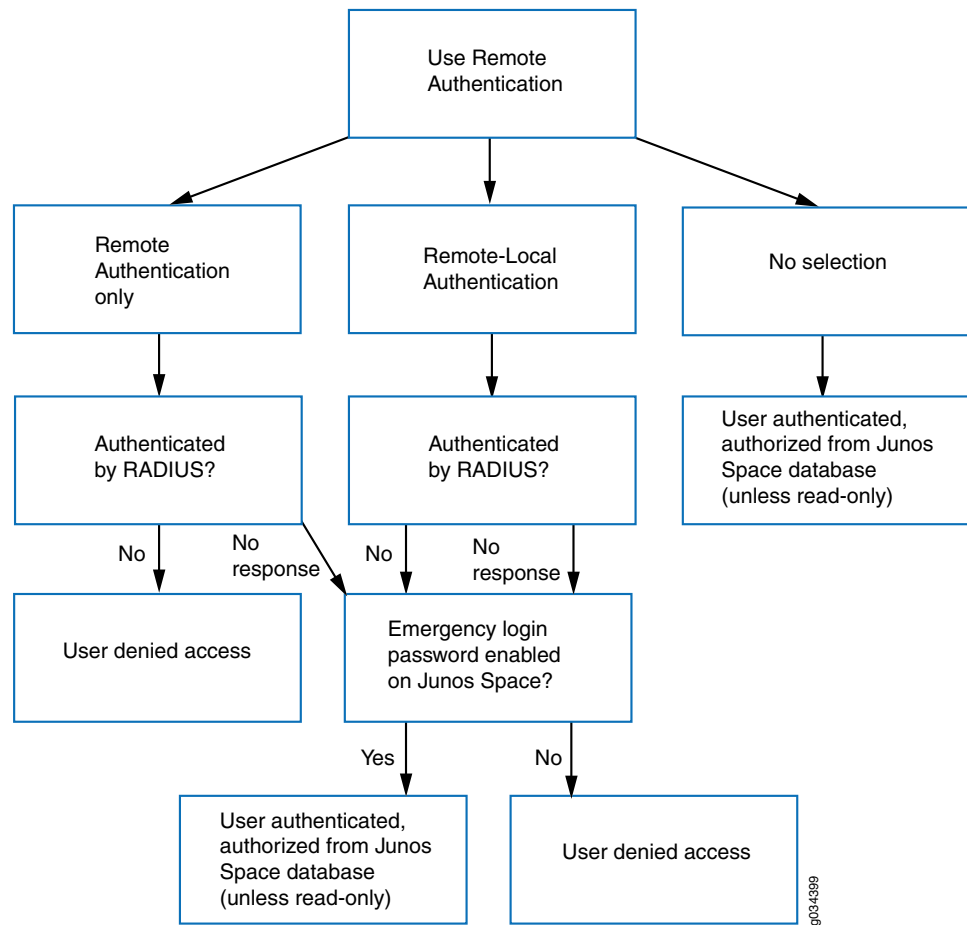


Figure 2 shows the results when a remote RADIUS server either rejects the user or does not respond at all.



Notes about the figures follow.

User is authenticated by RADIUS server

If the user is authenticated from one of the configured remote RADIUS servers, behavior is the same under both the remote-only and the remote-local options. One of two scenarios is true:

- The user does not exist in the Junos Space Network Management Platform database.

In this case, a new user (read-only) entity is created automatically by the system and added in the Junos Space Network Management Platform database. Two audit logs are generated, one showing the details of the remote profile assigned to the user, and another showing the details of the user login.

You cannot modify the read-only user to assign roles. This user is differentiated by a different icon on the Manage Users screen.

If any read-only user is removed from the RADIUS server, then you must manually remove that user from the Junos Space Network Management Platform database.

If no authorization information is present in the Access-Accept response from the RADIUS server, then the read-only user is authenticated with an empty set of roles.

- The user exists in the Junos Space Network Management Platform database.

If authorization information is present in the Access-Accept response from the RADIUS server, the user potentially has two sets of roles: the remote profile-to-role mapping from the remote RADIUS server, and the roles stored in the Junos Space Network Management Platform database. For authorization of this user, the remote profile-to-role mapping is used, rather than the Junos Space Network Management Platform database information.

If no authorization information is present in the Access-Accept response from the RADIUS server, the authorization information is picked up from the local Junos Space Network Management Platform database.

RADIUS server does not respond

If the RADIUS server is not responding and if the user exists in the Junos Space Network Management Platform database and any emergency login password is enabled for this user, the user is authenticated by Junos Space Network Management Platform and is authorized with the roles present in the local Junos Space Network Management Platform database. (This rule does not apply to read-only users.)

RADIUS server rejects the user

If the user is rejected by the remote RADIUS server:

- In the Remote Authentication Only case, the user is denied access.
- In the Remote-Local Authentication case, the result depends upon whether this user exists in the Junos Space Network Management Platform database and an emergency login password has been enabled for this user locally. If these conditions are not met, the user is denied access. If it has, the user is authenticated by Junos Space Network Management Platform and is authorized with the roles present in the local Junos Space Network Management Platform database. (This rule does not apply to read-only users.)

Related Documentation

- [Remote Authentication Overview on page 667](#)
- [Junos Space Authentication Modes Overview on page 668](#)
- [Managing Remote Authentication Servers on page 669](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)
- [Configuring TACACS+ for Authentication and Authorization on page 677](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Configuring TACACS+ for Authentication and Authorization

Junos Space Network Management Platform supports authentication and authorization of users from one or more TACACS+ servers. (A combination of TACACS+ and RADIUS servers is also supported.) If you configure multiple servers, they will be tried during authentication in the order listed in the user interface. If the first server accessed is not reachable or there is a shared-secret mismatch, the next one is tried. The results are the same as those described for RADIUS authentication and authorization.



NOTE: If you configure remote authentication using RADIUS or TACACS+, then the most restrictive concurrent session limit between the Junos Space server and the remote authentication server takes effect.

To add a TACACS+ remote authentication server:

1. Select **Administration > Auth Servers**.
2. In the Auth Mode Settings area, select the authentication method you want to use.

In local authentication mode, the controls for the Remote Authentication Server table are enabled so you can add authentication servers first and then switch to non-local authentication mode only when you are ready later. If you select the Use Remote Authentication check box, you can then select the Remote Authentication Only or the Remote-Local Authentication option.
3. Click **Save** to store the remote authentication mode setting you select.
4. In the Authentication Servers table, add a new remote authentication server by clicking Add (+).

The Create Auth Server dialog box appears.

5. Enter the required settings to connect Junos Space Network Management Platform to the TACACS+ remote authentication server. See [Table 101 on page 677](#).

Table 101: TACACS+ Remote Authentication Server Settings

Setting	Description
Server Type	The type of server to be added. Select TACACS+ to add TACACS+ as the remote server.
Server Name	The name of the server.
Protocol	The supported authentication protocols: <ul style="list-style-type: none"> • PAP—Password Authentication Protocol • CHAP—Challenge Handshake Authentication Protocol
IP Address	The IP address of the remote authentication server.
Port Number	The remote authentication server assigned TCP port number. The default is 49.

Table 101: TACACS+ Remote Authentication Server Settings (*continued*)

Setting	Description
Shared Secret	The text string that serves as a password between the TACACS+ server, proxy, and client.
Number of Tries	The number of retries that a device can attempt to contact a TACACS+ authentication server. The default is 3 tries.
Max Retry Timeout MSecs	The interval in milliseconds that Junos Space Network Management Platform waits for a reply from a remote authentication server. The default value is 6000.

6. In the Create Auth Server dialog box, click **OK**.
7. In the Manage Auth Servers page, click **Test Connection** to verify the Junos Space Network Management Platform connection to the remote authentication server.
 - If the test connection result is a success, the Remote Authentication Server is reachable.
 - If the test connection result is a failure, the Remote Authentication Server is unreachable.
 - If the test connection result displays the message "Mismatched Shared Secret," then the configured shared secret for that server is incorrect. Ensure that you have entered the correct remote authentication server shared secret details.

Configuring TACACS+ Authorization

Authorization data in the TACACS+ server are stored as attribute-value (A-V) pairs. The A-V pair contains the name of the remote profile. Therefore, you must configure users in the TACACS+ server with the A-V pair values corresponding to the remote profiles created in the Junos Space server to represent the user's roles.

When Junos Space Network Management Platform queries the TACACS+ server for user authorization, the TACACS+ server's junospace-exec service returns the remote profile name for that user. Junos Space Network Management Platform determines the user's role or roles from this response.

To assign roles to the user using the remote profile name, you can configure the network-management-profiles A-V pair for the junospace-exec service on the TACACS+ server. For example:

```

user = guestuser
{
  pap = cleartext "<password>"
  service = junospace-exec
  {
    network-management-profiles = guest_profile
  }
}

```

- Related Documentation**
- [Remote Authentication Overview on page 667](#)
 - [Junos Space Authentication Modes Overview on page 668](#)

- [Managing Remote Authentication Servers on page 669](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 673](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 679](#)

Junos Space Log In Behavior with Remote Authentication Enabled

This topic describes Junos Space Network Management Platform log in behavior with remote authentication only or remote-local authentication enabled.

Login Behavior with Remote Authentication Only Enabled



WARNING: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space Network Management Platform in a browser tab or window, make sure that tab or window was not previously used to surf a non-https website. Best practice is to close your browser and relaunch it before logging in to Junos Space Network Management Platform.

- The user logs in with the correct credentials:
 - As long as the user's password is on the remote server, login is successful.
 - If the first remote authentication server is present, log in success or failure solely depends on the password stored there, as no other servers are consulted. If the first authentication server is not reachable, the second server is connected in the order specified. If no authentication server is reachable, Junos Space Network Management Platform tries the local password in the Junos Space Network Management Platform database. If the password matches, the user logs in successfully.



NOTE: For remote authentication, most users should not have a local password. The local password in this case is for emergency purposes, when the remote authentication servers are unreachable.

- The user logs in with incorrect credentials or the user does not exist on the remote authentication server:
 - Access to Junos Space Network Management Platform is denied.



NOTE: Authentication servers, for security purposes, will not distinguish between these two cases. Therefore, Junos Space Network Management Platform must always treat these type of logins as an authentication failure. Once Junos Space Network Management Platform receives a response from an authentication server, the only options are immediate success or failure. No other servers are contacted.

- If no authentication servers are reachable, Junos Space Network Management Platform tries the local password. If the local password does not exist, or if the credentials do not match, logging into Junos Space Network Management Platform fails.
- The user attempts to log in but the remote server is down—See the previous two log in behaviors for details. Notify the Junos Space Network Management Platform administrator when a remote authentication server is down.
- The user attempts to log in when the remote authentication server has the correct credentials, but there is no equivalent user in Junos Space Network Management Platform. The user cannot log in to Junos Space Network Management Platform because there is no role information.
- The user attempts to log in when the remote authentication server is configured for Challenge/Response:
 - If the remote authentication server indicates a challenge is required, it provides the challenge question. Junos Space Network Management Platform displays the challenge question to the user on the Juniper login page, and waits for the user's response.
 - If the challenge question is answered correctly, it is possible that the authentication server may request additional challenges.
 - If the challenge question is answered incorrectly, it is possible that the authentication server may re-challenge the user with the same challenge, use a different challenge, or fail the login attempt completely. It is up to the authentication server configuration.
 - If the final challenge is answered correctly, the user logs in successfully.

Log In Behavior with Remote-Local Authentication Enabled



WARNING: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space Network Management Platform in a browser tab or window, make sure that tab or window was not previously used to surf a non-https website. Best practice is to close your browser and relaunch it before logging in to Junos Space Network Management Platform.

- The user logs in with the correct credentials—Junos Space Network Management Platform checks the remote authentication servers first. If authentication fails or if a server is unreachable, Junos Space Network Management Platform tries to authenticate locally. If there is a Junos Space Network Management Platform local password and the credentials match, the user logs in successfully.
- The user logs in with incorrect credentials— Junos Space Network Management Platform checks the remote authentication servers first. If authentication fails or if a server is unreachable, Junos Space Network Management Platform tries to authenticate locally. If there is a Junos Space Network Management Platform local password and the credentials match, the user logs in successfully.
- The user attempts to login but the remote server is down—Authentication occurs using only the local password. If the password exists and there is a match, the user logs in successfully. If the password does not exist and there is no match, the user does not log in successfully.
- The user attempts to login when the remote authentication server has the correct credentials, but there is no equivalent user in Junos Space Network Management Platform. The user cannot log in.
- The user attempts to login when the remote authentication server is configured for Challenge/Response:
 - If the remote authentication server indicates a challenge is required, it provides the challenge question. Junos Space Network Management Platform displays the challenge question to the user on the Junos Space login page, and waits for the user's response.
 - If the user answers challenge question correctly, it is possible that the authentication server may request additional challenges.
 - If the user answers challenge question correctly, it is possible that the authentication server may re-challenge the user with the same challenge, use a different challenge, or fail the login attempt completely. It is up to the authentication server configuration.
 - If the user answers challenge question correctly, log in is successful.

**Related
Documentation**

- [Remote Authentication Overview on page 667](#)
- [Logging In to Junos Space on page 3](#)
- [Junos Space Authentication Modes Overview on page 668](#)
- [Creating a Remote Authentication Server on page 670](#)
- [Modifying Authentication Settings on page 672](#)

CHAPTER 68

Manage SMTP Servers

- [Managing Platform SMTP Servers on page 683](#)
- [Adding a Platform SMTP Server on page 684](#)

Managing Platform SMTP Servers

You can configure one or several SMTP servers for use by Junos Space applications that need to transmit e-mail. For example, an application might use e-mail automatically to inform a support organization of an issue and might include logs or reports.

To configure and manage SMTP servers:

1. Select **Administration > SMTP Servers**.

The resulting screen lists all the configured servers. Only one can be the active server at one time. The active server is highlighted.

To add or delete an SMTP server:

1. Click the plus sign at the upper left of the screen to add a server.
2. Configure and add the server. See [“Adding an SMTP Server” on page 684](#).
3. To delete a server, click the X at the upper left of the screen.

To change the active SMTP server:

- Click the arrow at the upper left of the screen to select the server you want to make active.

The Test connection settings option is used to test the SMTP server connection from Junos Space Network Management Platform. It uses user (selected) defined port, authentication and security details when it tests the connection between the SMTP server and Junos Space Network Management Platform. To test the connection to the server:

- Click the **Test Connection** button at the upper-right corner of the screen.

If the SMTP server supports only TLS security protocol, the connectivity test succeeds for both the None and TLS security options. This is a known limitation in the connectivity test for testing the connection between the SMTP server and Junos Space Network Management Platform.

**Related
Documentation**

- [Adding an SMTP Server on page 684](#)

Adding a Platform SMTP Server

You can add an SMTP server to the list of configured servers to which applications can direct e-mail. To add an SMTP server, you must have administration privileges.

To add an SMTP server:

1. Select **Administration > SMTP Servers**.
2. In the resulting dialog box, click the plus sign in the upper-left corner.
The Create SMTP Server dialog box appears.
3. In the Server Name box, enter a name for the SMTP server, using alphanumeric values.
4. In the Host Address box, enter the IP address of the mail server.
5. Enter the port number.

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

6. In the From Email Address box, enter the e-mail address of this server.

This address will appear as the sender of e-mails from the applications that are using this server.

7. (Optional) If you want to use the SMTP Authentication security protocol to check the credentials of the sender, select **Use SMTP Authentication**.

When you select this option, the related username and password boxes are enabled.

8. (Optional) In the User Name box, enter the username that you want used for authentication.

9. (Optional) Enter the authentication password twice in the Password boxes to confirm it.
10. (Optional) If you want to use Transportation Layer Security (a cryptographic protocol) for further protection, select the **Use TLS** box.

Related Documentation

- [Managing SMTP Servers on page 683](#)

CHAPTER 69

Manage Tags

- [Overview on page 687](#)
- [Managing Tags on page 688](#)
- [Creating Tags on page 698](#)

Overview

- [Managing Tags Overview on page 687](#)

Managing Tags Overview

Use Manage Tags to view tag information, and create, share, rename, or delete them, as well as selecting devices..

There are three roles relevant to tags:

- To access Manage Tags and perform the above-mentioned tasks, you must have the System Administrator role. You can create public and private tags. You can also create hierarchies of tags.
- To share user-defined tags by publishing them so that others can use them, you must have the Tag Administrator role.
- Any Junos Space user can tag, view, apply, and untag objects.

Tag names should not start with space, cannot contain a comma, double quote, parentheses, and cannot exceed 255 characters.

To use Tags:

1. Create a private or shared tag using the **Network Management Platform > Administration > Manage Tags > Create Tag** user interface. See [“Creating a Tag” on page 698](#).
2. Tag an object on an inventory page. For example you can tag an object on the **Platform > Manage Devices** inventory page. Once you tag an object, you can view or untag existing tags. See [“Tagging an Object” on page 695](#) and [“Untagging Objects” on page 697](#).

3. (Optional) Create hierarchical tags and manage them in the Tag Hierarchy pane in the Tag view on an inventory landing page for taggable objects (such as devices). See [“Managing Hierarchical Tags” on page 689](#).
4. Manage tags using the **Platform > Administration > Manage tags** inventory page. You can share, rename, or delete tags. See [“Viewing Tags for a Managed Object” on page 696](#), [“Renaming Tags” on page 694](#), [“Deleting Tags” on page 695](#)

Related Documentation

- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)
- [Untagging Objects on page 697](#)
- [Filtering the Inventory by Using Tags on page 697](#)
- [Managing Hierarchical Tags on page 689](#)

Managing Tags

- [Managing Tags on page 688](#)
- [Managing Hierarchical Tags on page 689](#)
- [Sharing a Tag on page 693](#)
- [Renaming Tags on page 694](#)
- [Deleting Tags on page 695](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags on page 696](#)
- [Untagging Objects on page 697](#)
- [Filtering Inventory Using Tags on page 697](#)

Managing Tags

You can use tags to label and categorize objects in your network, such as subnets, devices, services, users, customers, and so forth so you can filter, monitor, or perform batch actions on them without having to select each object separately. You can also use tags to select devices. The inventory page allows you to manage and manipulate personal tags you created. You must have the System Administrator role to manage tags.

The Tags page is blank unless there are some public tags or private tags you created. Tags are only visible to you unless you have the Tag Administrator share them and make them public to all users. Tags created by other users are private and only visible to them unless the Tag Administrator shares them; making them public.

Manage all tags applied to inventory objects from the **Administration > Tags** inventory page. You can share, rename or delete tags. The Tags page is blank until you create one or more tags using the **Create Tag** icon.

Viewing Tags

To view tags on the inventory page:

- All tags appear on the inventory page in tabular view listed alphabetically by tag name.

You can filter inventory objects by a tag name (see [“Filtering the Inventory by Using Tags” on page 697](#)).

Viewing Tag Information

Tag data includes the tag name, access type, and the number of objects tagged by a particular tag. See [Table 102 on page 689](#).

Table 102: Tag Information

Tag Data	Description
Name	Unique tag name. Tag names cannot start with a space or be longer than 256 characters.
Access Type	Tags can either be public (shared) or private (visible only to the creator).
Tagged Object Count	The number of objects tagged in all workspace inventory pages by the tag.

You can sort and hide columns. For more information about manipulating tables in tabular view, see [“Junos Space User Interface Overview” on page 9](#).

Performing Actions on Tags

To perform an action on one or more tags:

1. Select one or more tags in the table.

Click a tag to select it. If you select one tag, you can perform all tag management actions. If you select two or more tags, you can only delete the tags.

2. Select a command from the Actions menu or right-click pop-up menu.

You can share (see [“Sharing a Tag” on page 693](#)), rename (see [“Renaming Tags” on page 694](#)), delete (see [“Deleting Tags” on page 695](#)), or deselect all selected tags.

Related Documentation

- [Tags Overview on page 687](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)
- [Untagging Objects on page 697](#)
- [Creating a Tag on page 698](#)

Managing Hierarchical Tags

Hierarchical tags consist of multiple levels of tags within a single tag. You can use hierarchical tags to classify objects managed by Junos Space Network Management Platform into categories and subcategories. Hierarchical tagging uses other tags to

classify a tag. The hierarchy allows you to drill down to the specific objects in Junos Space Network Management Platform very easily.

A hierarchical tag contains parent and child tags. For example, if you have an existing tag named West Coast and you create another tag within this tag named California, then the West Coast tag is the parent tag and the California tag is the child tag.

You can view, create, update, and delete hierarchical tags using the **Devices > Tags** inventory page.

The **Tags** inventory page displays all the objects on the network managed by Junos Space Network Management Platform using Tag and Tabular views.

You can use the Tag View icon to access this view. You can create and delete hierarchical tags as well as view them. You can also filter and display objects that are tagged with specific tags.

The Tag view is divided into two panes—Tag Hierarchy and Tabular View.

- Tag Hierarchy Pane—This pane appears on the left of the Tabular View pane. It displays a tree view of all the tags organized hierarchically.
 - Tabular View Pane—This pane appears on the right of the Tag Hierarchy pane. It displays a list of managed objects in a tabular form. If you select a particular tag in the tag hierarchy tree on the left, the objects associated with that particular tag are displayed in this pane.
- [Using the Tag Hierarchy Pane on page 690](#)
 - [Using the Tabular View Pane on page 693](#)

Using the Tag Hierarchy Pane

The Tag Hierarchy pane displays all tags organized hierarchically in a tree view. You can view, create, update, and delete tags in this pane.

To display the Tag Hierarchy pane, click the Tag View icon on the **Manage Devices** inventory page.

- [Using the Tag Action Bar on page 691](#)
- [Using the Right-Click Menu— on page 691](#)
- [Using Drag-and-Drop on page 692](#)
- [Using the Quick Info Tool Tip on page 692](#)
- [Browsing Tagged Objects on page 692](#)
- [Viewing All Tags on page 692](#)
- [Adding a Child Tag on page 693](#)
- [Deleting a Tag on page 693](#)
- [Using Notification on page 693](#)

Using the Tag Action Bar

You can use the Tag Action bar to add a child tag or delete an existing tag in the tag hierarchy tree. The Tag Action bar has two buttons—the plus [+] button and the minus [-] button. You can click the plus [+] button to add a child tag and the minus [-] button to delete a tag in the tag hierarchy tree.

To add a child tag:

1. Select the tag in the tag hierarchy tree for which you want to add a child tag.
2. Click the plus [+] button on the Tag Action bar.

The Add New or Existing Tag dialog box appears.

3. Type a new tag name in the text box, or use the magnifying glass search icon to search and select an existing public tag to add as a child tag.
4. Click the **Add Tag** button.

A new child tag is added to the tag hierarchy.

To delete a tag:

1. Select the tag you want to delete in the tag hierarchy tree.
2. Click the minus [-] button on the Tag Action bar.

If the selected tag appears in multiple locations, it is deleted from the current location.

If the selected tag appears in a single location only, then a confirmation dialog box prompts you to confirm the deletion.

Using the Right-Click Menu—

When you right-click a tag in the tag hierarchy tree, a right-click menu appears.

This menu displays the **Add Tag**, **Remove Tag**, and **Modify Tag** options. Use the **Add Tag** option to add a new child tag and the **Remove Tag** option to delete a tag.

To add a child tag using the right-click menu:

1. Right-click a tag in the tag hierarchy tree for which you want to add a child tag.

The right-click menu appears.

2. Click the **Add Tag** option on the right-click menu.

The Add New or Existing Tag dialog box appears.

3. Type a new tag name in the text box, or use the magnifying glass search icon to search and select an existing public tag to add as a child tag.
4. Click the **Add Tag** button.

A new child tag is added to the tag hierarchy.

To delete a tag using the right-click menu:

1. Select the tag you want to delete in the tag hierarchy tree.
2. Click the **Remove Tag** option on the right-click menu.

If the selected tag appears in multiple locations, it is deleted from the current location.

If the selected tag appears in a single location only, then a confirmation dialog box prompts you to confirm the deletion.

Using Drag-and-Drop

You can drag a tag from one location and drop it in another location to manipulate the tag hierarchy. When you drag and drop a tag from one location to another, the corresponding tagged objects are not affected. For example, If the tag is associated with five devices, then it remains associated with the same five devices after you drag and drop the tag from one location to another.

Using the Quick Info Tool Tip

The Quick Info tool tip provides quick and immediate statistics about a tag. You can drag the mouse over a tag name or a tag icon in the tag hierarchy tree to get a quick summary about its tagged objects.

To view the tool tip for a tag:

1. Select a particular tag in the tag hierarchy tree.
2. Drag the mouse over the tag icon or the tag name.

Brief statistics about the tagged objects appear.

Browsing Tagged Objects

When you browse the tag hierarchy tree and select a tag, the corresponding tagged objects appear in the Tabular View pane. When you select the root node in the tag hierarchy tree, all tagged objects appear in the Tabular View pane without any filtering.

You can click the [X] icon in the Tabular View pane to clear tag filtering. When you clear tag filtering, the root node in the tag hierarchy tree is automatically selected and all tagged objects appear in the Tabular View pane.

Viewing All Tags

By default, the tag hierarchy tree displays tags relevant to the **Manage Devices** inventory page only. In this mode, only those tags appear that are either empty or that tag at least one object on the inventory page.

You can also view all public tags in the tag hierarchy tree.

To view all public tags:

1. Navigate to the Tags toolbar at the top of the Tag Hierarchy pane.
2. Select the **Show All Tags** option from the Tags list.

All public tags appear in the Tabular View pane on the right.

Adding a Child Tag

You can use either the Tag Action bar or the right-click menu to add a child tag to the tag hierarchy tree. To add a child tag using the Tag Action bar, see [“Using the Tag Action Bar” on page 691](#). To add a child tag using the right-click menu, see [“Using the Right-Click Menu—” on page 691](#).

Deleting a Tag

You can use either the Tag Action bar or the right-click menu to delete a tag from the tag hierarchy tree. To delete a tag using the Tag Action bar, see [“Using the Tag Action Bar” on page 691](#). To delete a tag using the right-click menu, see [“Using the Right-Click Menu—” on page 691](#).

Using Notification

When multiple Junos Space Network Management Platform users view the same tag view on the **Manage Devices** inventory page, any change a user makes is immediately updated in the other tag views. Changes include creating, updating, and deleting tags in the Tag View pane, and tagging objects in the Tabular View pane.

Using the Tabular View Pane

The Tabular View pane displays all managed objects as rows in a table. When you select a particular tag in the tag hierarchy tree, its corresponding tagged objects are displayed in this pane.

In this view, you can tag objects and also search for objects tagged with a particular tag.

Tagging an object using a hierarchical tag in the Tabular View pane is similar to tagging an object using a nonhierarchical tag on any application workspace manage inventory page. For information on how to tag an object, see [“Tagging an Object” on page 695](#).

To search for specific tagged objects:

1. Navigate to the Devices page.
2. Select a public tag in the search box.

The tag hierarchy tree automatically navigates to the selected tag, and the Tabular View pane displays the objects tagged with that particular tag only.

Related Documentation

- [Tags Overview on page 687](#)

Sharing a Tag

User-defined tags are always created as private tags initially. When you feel that your tag has public value, sharing a tag makes it public for all users to use it to tag objects on a workspace inventory page. To share a tag, you must have Tag Administrator privileges.

To share a tag.

1. Select **Administration > Tags**.

The **Tags** inventory page is displayed.

2. Select one or more private tags on the inventory page.
3. Select **Share Tag** from the Actions menu or right-click to select **Share Tag** from the pop-up menu.

The **Share Tag** status box appears to indicate whether the tag sharing is successful.

You can also share a tag when you create one (see [“Creating a Tag” on page 698](#)).

4. Click **OK**.

The tag **Access Type** changes on the inventory table from **private** to **public**.

Related Documentation

- [Tags Overview on page 687](#)
- [Managing Tags on page 688](#)
- [Renaming Tags on page 694](#)
- [Deleting Tags on page 695](#)
- [Creating a Tag on page 698](#)

Renaming Tags

The Rename Tag command provides you flexibility to reorganize or recategorize managed objects according to your changing needs.

To rename a tag:

1. Select **Administration > Tags** inventory page.
2. Select the tag you want to rename.
3. Select **Rename Tag** from the Actions menu.

The **Rename Tag** dialog box appears.

4. Type a tag name in the **New Name** text field.

A tag name should not start with a space, cannot contain a comma, double quote, parentheses, or exceed 255 characters

5. Click **Rename**.

The old tag is renamed and saved in the database. You see the renamed tag in the inventory page.

When you navigate to the manage inventory page from which you created the tag, you will see the renamed tag name in the Actions > **View Tags** dialog box and in the search list.

- Related Documentation**
- [Tags Overview on page 687](#)
 - [Managing Tags on page 688](#)
 - [Sharing a Tag on page 693](#)
 - [Deleting Tags on page 695](#)
 - [Creating a Tag on page 698](#)
 - [Filtering the Inventory by Using Tags on page 697.](#)

Deleting Tags

Use the Delete Tags action to remove managed object tags you no longer need.

To delete a tag:

1. Select **Administration** > **Tags** inventory page.
The **View Tags** page appears.
2. In the **View Tags** table, select one or more tags you want to delete.
3. Select **Delete Tag** from the Actions menu. You can also right-click the selected inventory object(s) and select **Delete Tags** from the pop-up menu.

The **Delete Tags** dialog box appears to confirm that you want to delete the tag.

4. Click **Delete**.

The tag is removed from the database and no longer appears in the View Tags table.

- Related Documentation**
- [Tags Overview on page 687](#)
 - [Managing Tags on page 688](#)
 - [Sharing a Tag on page 693](#)
 - [Renaming Tags on page 694](#)
 - [Creating a Tag on page 698](#)

Tagging an Object

You can create user-defined tags in an application workspace inventory page to easily categorize and organize managed objects. Subsequently, you can view and use these tags to easily search for multiple objects to view status or perform a bulk action on them without having to select each individually.

To tag an object:

1. Navigate to an application workspace manage inventory page. For example, select **Devices** > **Device Management**.
2. Select the inventory object(s) you want to tag.
3. Select **Tag It** from the Actions menu.

The **Apply Tag** dialog box appears.

4. Select or type the tag name in the text box.

If you have existing tags, start to type a tag name in the name field. Existing tags appear in the selection box.

5. Click **Apply Tag**. This action tags the object and stores the tag in the database.

**Related
Documentation**

- [Tags Overview on page 687](#)
- [Managing Tags on page 688](#)
- [Viewing Tags for a Managed Object on page 696](#)
- [Untagging Objects on page 697](#)
- [Filtering the Inventory by Using Tags on page 697](#)
- [Creating a Tag on page 698](#)

Viewing Tags

The View Tags action from application workspace inventory pages allows you to see all of the tags that you have assigned a managed object on your network. You must first tag a managed object to see its tags.

Use tags to label and categorize objects in your network, such as subnets, devices, services, users, customers, and so forth so you can filter, monitor, or perform batch actions on them without having to select each object separately.

Tags created by you are private and only visible to you unless you have the Tag Administrator share them to the public domain, making them public. Tags created by other users are only visible to them unless the Tag Administrator shares them, then you can view them.

To view tags on an inventory object:

1. Navigate to a workspace inventory page.
2. Select only one inventory object for which you want to view tags.
3. Select **View Tags** from the Actions menu. You can also right-click an object and select **View Tags** from the pop-up menu.

The **View Tags** dialog box appears with a tag list displaying all tags applied to the selected object.

4. Click **OK**.

**Related
Documentation**

- [Managing Tags on page 688](#)
- [Tagging an Object on page 695](#)
- [Untagging Objects on page 697](#)

Untagging Objects

You can untag or remove a tag from an object on a workspace inventory page. You can only select one object at a time to untag.

To untag an object:

1. Navigate to a workspace inventory page. For example, select **Devices > Device Management**.
2. Select one object on the workspace inventory page at a time.
3. Select **UnTag It** in the Actions menu or right-click an object and select **UnTag It** from the pop-up menu.

The **UnTag The Object** dialog box appears.

4. Select the tags that you want to remove.
5. Click **Untag**.

The Untag dialog box appears displaying that the object has been successfully untagged.

6. Click **OK**.

In this example, you are returned to the Device Management workspace.

Related Documentation

- [Tags Overview on page 687](#)
- [Managing Tags on page 688](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)
- [Creating a Tag on page 698](#)

Filtering Inventory Using Tags

You can use tags to filter objects on a workspace inventory page. Filtering allows you to view only the objects that you want categorized by the tag name.

To filter using a tag:

1. On the workspace inventory page, click the magnifying glass in the search field at the top-right of the page. You can also type the first letter of the tag name.

The list appears with the object names on the top and the tag names on the bottom. (If you clicked a letter in the search field, only the tag names starting with that letter would appear.)

2. Click a tag name in the list.

Only the inventory objects with that tag name appear. You see **Filtered By the tag** name at the top-left of the page.

3. Click the red **X** to remove the filtering from the inventory page.

In another aspect of filtering, on some pages, you can see a preview of the tagged objects you selected. For example, in the Configuration Files workspace, in **Configuration Files > Config Files Management > Backup Config Files**, you can select devices by tags. This form of filtering enables you to verify that you are performing the current operation on the correct objects.

Related Documentation

- [Tags Overview on page 687](#)
- [Managing Tags on page 688](#)
- [Tagging an Object on page 695](#)
- [Viewing Tags for a Managed Object on page 696](#)
- [Untagging Objects on page 697](#)
- [Creating a Tag on page 698](#)

Creating Tags

- [Creating a Tag on page 698](#)

Creating a Tag

To create a tag:

1. Select **Administration > Tags** and select the **Create Tag** icon.

The **Create Tag** dialog box appears.

2. If necessary select the **Share this Tag** option.

When you share a tag, all users can use that tag. Only the Tag Administrator can publish tags to the public domain.

3. Type a tag name in the text box.

A tag name should not:

- Exceed 255 characters
- Start with a space
- Contain special characters, such as commas, double quotes, parentheses, or question marks.

4. Click **Create**.

The Create Tag dialog box appears displaying that the tag is successfully created.

5. Click **OK**.

The tag appears in the **Tags** inventory page. If the tag is shared it is public; if not it is private.

- Related Documentation**
- [Tags Overview on page 687](#)
 - [Managing Tags on page 688](#)
 - [Sharing a Tag on page 693](#)
 - [Renaming Tags on page 694](#)
 - [Deleting Tags on page 695](#)

CHAPTER 70

Manage Permission Labels

- [Managing Permission Labels Overview on page 701](#)
- [Understanding Subobject-Level Access Control on page 704](#)
- [Working With Permission Labels on page 705](#)

Managing Permission Labels Overview

Permission Label is the tool by which you can enforce object-level and subobject-level access control; for example, you can restrict a user with the role of Device Manager to a subset of devices that you choose or to only specific parts of the chosen devices.

Permission Labeling enables you to define users' access to objects or subobjects in—or elements of—Junos Space Network Management Platform. These objects can be users, roles, profiles, configlets, scripts, or devices. For Junos Space Release 13.1, the subobjects belong to the device category and can be the physical or logical interfaces, or the physical inventory of the devices. Prior to the release of Junos Space 11.3, access was associated solely with roles. It was the role that defined the elements a user could access; for example, a Device Admin could access the Devices workspace, and work with all the devices there. Using Permission Labels enables you to restrict a user's access to subordinate parts of the elements associated with his or her role.

You can now confer the Device Admin role on a user, and then assign a permission label to that user to restrict him or her to managing only devices with the same label, as opposed to all the devices in Junos Space Network Management Platform.

Similarly, you can attach a permission label to the users in a particular location (for example, San Francisco), and assign the same label to a user administrator. Provided all the users in other locations are also labeled—but differently—that user administrator's activities are confined to managing users in San Francisco.

The same principle applies to roles. You can attach a label to the roles for managing other applications, such as Service Now or Network Activate, and then assign the same label to appropriately qualified users.

You can assign a permission label to configlets and then assign that label to the user so that the user could work on only those configlets assigned to them. You could also assign a permission label to templates and template definitions and assign that label to users.

Only, those users who have been assigned the permission label can work on the templates and template definitions.

Similarly, the user could also be restricted from using all the scripts. This can be done by assigning permission label to certain scripts and then assigning that label to the user. When the user tries to access the script, they will be presented with only the script assigned to them through the permission label.



NOTE: Until Junos Space Release 13.1, if the users had access to an object, then they automatically had access to its subobjects as well. From Junos Space Release 13.1, you can restrict users to have access to only the subobjects instead of the entire object. For example, you can restrict a user to have access to only certain interfaces on a device.

Working with permission labels is a three step process, involving the creation of a label, assigning that label to a user, and attaching that label to an object. You can choose not to use permission labels at all. However, once you decide to implement them, they have an effect on all users and objects, in that labeling an object immediately restricts it to viewing by users with the same label. Only users with the appropriate roles can manipulate objects in Junos Space Network Management Platform, and without the appropriate distribution of permission labels *in addition*, even users with the appropriate roles cannot see labeled objects.

These are the possible combinations:

- If you do not assign a label to a user, that user can see all the unlabeled objects necessary to perform the tasks associated with his or her role.
- If you assign a label to a user, but do not attach the same label to any objects, the effect is the same as above.
- If you do not attach a label to an object, all users with the appropriate role can see that object.
- If you attach a label to an object, only users to whom the same label has been assigned, and who have the appropriate role can see and access that object.

Examples of labeling discrepancies:

- You attach a label to some of your devices, but you forget to assign that label to any users. Result: only users with the Permission Label Manager role can see those devices.
- You attach a “UK” label to all your devices, but you assign the device manager user who is supposed to manage them the “London” label. Result: the device manager cannot even see the devices.
- You attach the “Bengaluru” permission label to some of your devices. You assign the same label to the person who is supposed to manage *only* those devices, not the devices in Chennai. You forget to label the Chennai devices. Result: the device manager in Bengaluru can see all the devices, but *only* he or she can see the Bengaluru devices.

Both objects and users can have multiple permission labels that can be assigned and attached or removed at any time. (However, a user who is both a Permission Label Manager and a Device Administrator can execute operations only on devices.)



NOTE: If a system is upgraded from a previous release to 11.3, all elements are global by default (no permission labels applied), and users have no pre-assigned permission labels. The Super Administrator can execute all the new Permission Label tasks.

Because assigning permission labels amounts to controlling access, it requires a special role, Permission Label Administrator. Any user who can perform this task can see all the labels for all the objects appropriate to his or her other roles. In other words, to label configuration files, you also need to have the Configuration File Manager role. To the Permission Label Administrator role belong three tasks:

- Design permission label—Create and delete permission labels.
- Assign permission label—Assign permission labels to users
- Attach permission label—Attach permission labels to objects

Instructions for performing these three tasks are in [“Assigning Permission Labels” on page 705](#). You might wish to separate these tasks because you might not want a user to create an object such as a device, label it, and then ensure only he or she has access to that object.

Operations with permission labels generate Audit Log entries, showing not only the usual level of detail with the task performed, etc., but also information about the person who performed the task:

- Login ID
- First name
- Last name
- Email address
- Assigned role

**Related
Documentation**

- [Understanding Subobject-Level Access Control on page 704](#)
- [Assigning Permission Labels on page 705](#)
- [Role-Based Access Control Overview on page 479](#)
- [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)
- [Predefined Roles Overview on page 481](#)

Understanding Subobject-Level Access Control

Until Junos Space Release 13.1, you have been able to restrict users to a set of objects by assigning permission labels to the objects. However, as an administrator who needs a higher-level of granularity, you may want to ensure that users are assigned rights to manage only specific components within an object. For example, you may want to restrict the access of certain users to specific interfaces, subinterfaces, and so on within a device. To meet this requirement, from Junos Space Release 13.1 onward, you can assign permission labels to various subobjects or components within an object. Using this feature, for example, you can assign a permission label to the physical interface ge/0/0 on Device 1 and physical interface ge/1/2 on Device 3. When you assign the same label to a user, the user can access only the interfaces ge/0/0 and ge/1/2, and cannot access any other components of the devices. “Device 1” and “Device 3” are just examples and represent random devices.

For Junos Space Release 13.1, the only object type that is supported for subobject-level access control is the device category. You can restrict user access to the following components of a device:

- Physical interfaces
- Logical interfaces
- Physical inventory, such as operations on the Routing Engine, port, and so on

If a user is assigned multiple permission labels, the effects are additive, just as they are with object-level access control. For example, if you have assigned PL-1 (label name) to interface A on Device 1 and PL-2 (label name) to interface B on Device 1, and then assign PL-1 and PL-2 to a user, then the user has access to interfaces A and B on Device 1.

To assign permission labels to subobjects, the configuration workflow requires that you first choose a device and then choose the subobjects for each of those devices. For more information about assigning permission labels, see [“Assigning Permission Labels” on page 705](#).

A subobject is not displayed on the inventory landing pages (ILPs) if a user does not have access to it.

Subobjects Dependencies

If there is a dependency between one subobject (parent) and another subobject (child), the following behavior can be expected:

- When you assign a permission label to a parent subobject, then:
 - All the child subobjects are labeled with the same permission label, including any child subobject that is subsequently created.

For example, if you assign a label to a physical interface, then the same label is automatically assigned to all the logical interfaces belonging to that physical interface. Similarly, the labels that you assign to a PIC are assigned to its child object, ports.

- For Junos Space Release 13.1, the administrator cannot deselect any of the child subobjects. That is, full access to the parent automatically enforces full access to all the children.

For this release, no parent–child relationship is enforced between ports and physical interfaces.

- When you assign a permission label to a child subobject without assigning the label to its parent, then:
 - Where the objects are visible in tree-form (for example, View Physical Inventory, Modify Device Configuration), the parent node will be visible but:
 - The parent object is read-only
 - No attributes of the parent object and no child objects are visible, except for the child subobject to which the permission label is assigned
 - Where the objects are visible as top-level objects in a grid (for example, View Physical Interfaces and View Logical Interfaces), the parent object is not visible



NOTE: If the user does not have access to a subobject (for example, a physical interface) but has access to its child subobject (one of its logical interfaces), then the parent subobject is displayed on the ILPs but none of its attributes or its child subobjects are visible, except for the child subobject to which the user has access.

**Related
Documentation**

- [Assigning Permission Labels on page 705](#)
- [Managing Permission Labels Overview on page 701](#)

Working With Permission Labels

From an efficiency perspective, it works best to create all your permission labels at once. Therefore, before you begin, it is best to map out what you intend to do, so that you can correctly match up permission labels with objects (or subobjects) and users. For a discussion of the consequences of mismatching them, see “[Managing Permission Labels Overview](#)” on page 701.

Once you have created your permission labels, you assign them to users and attach them to objects and subobjects. The sequence in which you assign and attach does not matter.

These instructions assume you have prepared your mapping, and that the users to whom you will assign permission labels already have the appropriate roles (see “[Configuring Users to Manage Objects in Junos Space Overview](#)” on page 480).

Objects, subobjects, and users can have multiple permission labels that can be assigned and attached or removed at any time.

The following topics provide information about how to create and assign permission labels to objects, subobjects, and users:

1. [Creating Permission Labels on page 706](#)
2. [Assigning Permission Labels to Users on page 706](#)
3. [Attaching Permission Labels to Objects on page 707](#)
4. [Managing Subobjects on page 709](#)

Creating Permission Labels

Note that you can only create, delete, or rename permission labels if your role includes the Design Permission Label task (see [“Role-Based Access Control Overview” on page 479](#)).

To create a permission label:

1. Select **Administration > Permission Labels** and select the **Create Permission Label** icon.

The Create Perm Label dialog box appears.

2. In the **Label name** box, enter an alphanumeric name. Spaces are acceptable, if not desirable.
3. Click **Create**.

The Create Permission Label dialog box appears stating whether the permission label is created successfully.

4. Click **OK** on the Create Permission Label dialog box.

You are returned to the Permission Labels page and the newly added permission label is displayed on this page.

You can rename or delete a permission label by selecting the label on the Permission Labels page and clicking the **Modify Permission Label** or **Delete Permission Labels** icon, respectively.



.....
NOTE: Every instance of a label is renamed. Users assigned the old label now automatically have the new, renamed label.
.....

Assigning Permission Labels to Users

Note that you can only assign permission labels to users or remove them from users if your role includes the Assign Permission Label task (see [“Role-Based Access Control Overview” on page 479](#)).

To assign a permission label to a user:

1. Select **Administration > Permission Labels**.

The Permission Labels page appears.

2. Select the permission label you want to assign and select **Assign Permission Labels to Users** from the Actions menu.

The Assign Permission Labels to Users page appears.

3. Select the appropriate user(s). To page through the table, use the controls on the status bar at the bottom of the table. This page also shows the total number of pages of records, the current page being displayed, and the number of items per page, which can be adjusted.

To search for a user, enter the username in the search field and then press **Enter** or click the magnifying glass icon adjacent to the search field. All users matching the search criteria appear on the search results page. Click the cross icon next to the search results to clear the search results.

The following information appears for each user: login IDs, their last and first names, and the permission labels already assigned to them.

4. Click **Assign**.

The Permission Labels page reappears, displaying the label name with the Assigned Users Count adjusted to reflect the number of users assigned to the label.

You can un-assign or remove a permission label from a user by selecting the label on the Permission Labels page and selecting **Remove Permission Labels from Users** from the Actions menu. Only one label at a time can be removed, although you can remove it from multiple users at the same time.

Attaching Permission Labels to Objects

In the context of permission labels, objects can be devices, profile, role, configlets, scripts, Service Now devices and users. The subobjects can be the physical or logical interfaces, or the physical inventory of a device.

Note that you can only assign permission labels or remove them from objects or subobjects if your role includes the Attach Permission Label task (see [“Role-Based Access Control Overview” on page 479](#)).

To attach a permission label to an object:

1. Select **Administration > Permission Labels** and select the **Create Permission Label** icon.

The Permission Labels page appears.

2. Select the permission label you want to assign, and select **Attach/Detach Permission Label to Objects** from the Actions menu.

The Attach/Detach Permission Label to Objects page appears. On the left, it displays a list of object types. On the right, it displays the list of objects belonging to the selected object type to which the label has been previously attached. If no labels have yet been attached, these lists are empty. For example, when you start initially, the right-hand side of this page is usually empty indicating that objects are yet to be attached to this label.

3. If the object type that you want is not listed on the Attach/Detach Permission Label to Objects page, click the **Add Managed Object Type** icon to add the required object type (that is, click the plus icon that is toward the far left-hand side of this page).

The object types that are supported are:

- **CLI Configlet Object**—Object type to assign a permission label for CLI configlet.
- **Configuration View Filter Object**—Object type to assign a permission label for specific objects within the configuration object. For example, you can assign a permission label to the firewall object within the configuration object (that is, the objects that you filter from Devices > Device Management > View Active Configuration).
- **Configuration Viewer Object**—Object type to assign a permission label for configuration objects (that is, the objects that you view from Devices > Device Management > View Active Configuration).
- **Device Object**—Object type to assign a permission label for device objects.
- **Device Script Object**—Object type to assign a permission label for device script objects.
- **Profile Object**—Object type to assign a permission label for remote profiles.
- **Role Object**—Object type to assign a permission label for RBAC (Role-based access control) Role, which actually means any role.
- **Template Definition Object**—Managed object type to assign permission label for template definition objects.
- **Template Object**—Managed object type to assign a permission label for template objects.
- **User Object**—Managed object type to assign a permission label for administrator user.

The **Add More Object Types** dialog box appears, displaying the names of the objects not yet in the table and their descriptions.

4. Select one or more object types and click **OK**.

The Attach/Detach Permission Label to Objects page reappears and displays the newly added object type..

5. To select specific objects to which a label is to be attached:
 - a. Select the object type from the left-pane of the Attach/Detach Permission Label to Objects page.

For example, select **Device Object**.

- b. If no objects are displayed or you do not see the objects to which you want to attach a label:

1. Click **Add Managed Objects**.

The Add More Objects page appears listing all the objects to which you can attach the label. To page through the table, use the controls on the status bar at the bottom of the table. This page also shows the total number of pages of records, the current page being displayed, and the number of items per page, which can be adjusted. In the example, because you have selected Device Object, this page displays all the objects that have been discovered from Junos Space.

To search for an object, type the object name in the search field and then press **Enter** or click the magnifying glass icon adjacent to the search field. All objects matching the search criteria appear on the search results page. Click the cross icon next to the search results to clear the search results.

You can also select the **Show Only Objects without Permission Label** check box to display the objects without any permission labels attached to them.

2. Select the objects to which you want to assign the label.
3. Click **OK**.

The Attach/Detach Permission Label to Objects page reappears displaying the newly added objects.

- c. Select the objects to which you want to attach a label.

The bottom of the page displays the total number of pages of records, the current page being displayed, and the number of items per page, which can be adjusted. Use the controls provided to navigate to the previous or next page.

- d. Click **OK**.

The Attach/Detach Permission Label to Objects page reappears, now displaying the type of object plus the individual objects you selected in the last step. The Labels Attached column displays the new label that you attached.

6. Click **Close**.

You are returned to the Permission Labels page.

To detach or remove a permission label from an object:

1. From the Attach/Detach Permission Label to Objects page, select the object type.

The right pane of the page displays the objects of the selected object type to which the label is attached.

2. Select the objects.
3. Click the **Remove Managed Objects** icon.

The Remove Objects from Permission Label page appears listing the objects from which the label should be removed.

4. Click **Remove**.

You are returned to the Attach/Detach Permission Label to Objects page and you can see that the deleted objects are no longer listed.

Managing Subobjects

From Junos Space Release 13.1 onward, you can restrict user access to specific components or subobjects within an object. You can accomplish this task by selecting the objects first and then choosing the subobjects for each of those devices and assigning the permission labels to these subobjects.

To assign a permission label to a subobject:

1. Select **Administration > Permission Labels**.

The Permission Labels page appears.

2. Select the permission label.

You can select only one permission label at a time.

3. Click **Attach/Detach Permission Label to Object**.

The Attach/Detach Permission label to Objects page appears.

4. Select the object type to view the objects of that type to which the selected permission label should be attached.

5. Select the objects. If no objects are listed, perform step 5 of the “Attaching Permission Labels to Objects” procedure.

6. Click **Manage Sub Objects**. For Junos Space Release 13.1, subobjects are supported only for the Device Object type.

The Manage Sub Object page appears listing the subobjects of all the selected devices. The subobjects of a device are categorized into **Physical Interface** subobjects, **Logical Interface** subobjects, and **Physical Inventory** subobjects.

7. Perform one of the following steps:

- Retain the selection of the **Entire Device** option if you want to assign the selected permission label to all the subobjects of all the selected devices. Although you can view all the subobjects, you cannot select any individual subobject. Go to step 11 to complete the task of assigning permission labels to all the subobjects.
- Select **Sub-Level Objects of Device** if you want to assign the selected permission label to specific subobjects.

8. From the **Physical Interfaces** tab, select all the physical interfaces to which you want to assign the permission label.

By default, the interfaces are grouped by device.

The selected subobjects are displayed on the right pane of the Manage Sub Object page under Selected Sub Object.



NOTE: When you select a physical interface, all the logical interfaces associated with this physical interface are automatically selected. The **Number of Logical Interfaces Selected** column displays this information. Click the link that appears below this column to view all the logical interfaces associated with the selected physical interface.

You cannot deselect these logical interfaces from the Logical Interface tab. Any logical interfaces that are later created for this physical interface are also assigned this label. You can deselect only the physical interfaces which in turn will deselect the logical interfaces associated with this physical interface. To select the logical interfaces separately, use the Logical Interfaces tab.

9. From the **Logical Interfaces** tab, select all the logical interfaces to which you want to assign the permission label.

The selected subobjects are displayed on the right pane of the Manage Sub Object page under Selected Sub Object.



NOTE: If you selected a physical interface from the Physical Interfaces tab, then by default all the logical interfaces associated with this physical interface are selected. You cannot deselect these logical interfaces from the Logical Interfaces tab.

10. From the **Physical Inventory** tab, select all the physical inventory objects to which you want to assign the permission label.

The selected subobjects are displayed on the right pane of the Manage Sub Object page under Selected Sub Object.

11. Click **OK**.

The selected permission label is assigned to all the selected subobjects.

After the objects and subobjects have been assigned successfully to a user, when the user logs in, the Device Management ILP and the global search results display only the objects and subobjects to which the user has access.

Related Documentation

- [Understanding Subobject-Level Access Control on page 704](#)
- [Managing Permission Labels Overview on page 701](#)
- [Role-Based Access Control Overview on page 479](#)
- [Configuring Users to Manage Objects in Junos Space Overview on page 480](#)

CHAPTER 71

Manage DMI Schemas

- [Managing DMI Schemas Overview on page 714](#)
- [Updating a DMI Schema on page 716](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 719](#)
- [Setting a Default DMI Schema on page 722](#)
- [Troubleshooting DMI Schema Management on page 723](#)

Managing DMI Schemas Overview

To manage multiple DMI schemas (device management interface schemas) for Junos-based device families and device types, use the DMI schema management workspace.

Each device type is described by a unique data model (DM) that contains all the configuration data for it. The DMI schema lists all the possible fields and attributes for a type of device. The newer schemas describe the new features coming out with recent device releases. It is important that you load into Junos Space Network Management Platform all your device schemas, otherwise only a default schema will be applied when you try to edit a device configuration using the device configuration edit action in the Devices workspace (see [“Modifying Device Configuration Overview” on page 53](#)). If Junos Space Network Management Platform has exactly the right DMI schema for each of your devices, you can access all of the configuration options specific to each device.

The DMI Schema Management workspace enables you to add or update schemas for all Junos Space devices. It also lets you know when you do not have the schema for a device. On the Manage DMI Schemas page, in the tabular view, when it says under the column DMI Schema "Need Import" it means the Junos OS schema for that device OS is not bundled with Space and you need to download it from the Juniper Schema Repository.

An important aspect of schema management is setting a default DMI schema for each device family. When you create a device template, the template needs a default schema for the device family. Conversely, in order to access all the configuration options for a particular device via the Edit Device Configuration action in the Devices workspace, you need to have the DMI schema specific to that device.

The schema management facility enables you to connect with Juniper's SVN Repository so that you can download new schemas as necessary.



NOTE: Ensure that you only download device schemas pertaining to the devices that are currently managed from Junos Space. As and when more devices are added, you can download the device schemas that are relevant to the newly added devices.

A schema is delivered in the form of a .tgz file, an archive containing multiple files reflecting the configuration hierarchy for the selected device family, platform and OS version. You can even create your own tgz file (see [“Creating a Compressed Tar File for Updating DMI Schema” on page 719](#)).

A typical goal in the DMI Management workspace—**Manage DMI Schemas**—is to enable a device to be managed in Junos Space Network Management Platform.

For each DMI schema currently installed, the **Manage DMI Schemas** inventory landing page displays:

- Name
- Device Family
- OS Version
- Device Series
- State—default or otherwise

You can view the schemas in tabular form, and you can sort the schemas by clicking on their column headings.

You can select one or more schemas and perform the following actions on them using the Actions menu or the right mouse-click menu:

- Set default schemas

Do this to return a custom configuration of a DMI schema to the default.

- Tag and untag schemas
- View schema tags, with
 - Tag Name
 - Access Type

To add or update a DMI schema, see [“Updating a DMI Schema” on page 716](#).

**Related
Documentation**

- [Updating a DMI Schema on page 716](#)
- [Setting a Default DMI Schema on page 722](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 719](#)
- [Troubleshooting DMI Schema Management on page 723](#)
- [Device Discovery Overview on page 131](#)
- [Add Deployed Devices Wizard Overview on page 141](#)

Updating a DMI Schema

To add or update a DMI schema, you must have the .tgz archive containing it on the machine running the Junos Space GUI. There are several ways of acquiring such files. You can:

- Create your own file (see [“Creating a Compressed Tar File for Updating DMI Schema” on page 719](#)).
- Download a file from Juniper’s SVN Repository. This topic contains the instructions for doing this.
- Get a file from Juniper support staff.

From the **Schema Update** page, Junos Space Network Management Platform is able to identify which schemas you already have installed, and based on the discovered devices, also suggests new schemas. You can, however, pick other available schemas and download them as well, or instead.

On the **Schema Update** page, you can either:

- Install a DMI schema on Junos Space Network Management Platform using a file you already have on the machine running the Junos Space GUI.

Or:

- Get a DMI schema from Juniper and update Junos Space Network Management Platform, which involves the following sub-tasks:
 - Configure a connection to the SVN Repository.
 - Connect to the SVN Repository and install DMI schemas on Junos Space Network Management Platform.

To install a DMI schema update on Junos Space Network Management Platform:

Select **Administration > DMI Schemas** and select the Update Schema icon.

The **Update Schema** page appears.

If you already have the tgz file on your system:

1. Select the **Archive (tgz)** option button.
2. Click **Browse**.

The **File Upload** dialog appears.

3. Navigate to the .tgz file and select it. Click **Open**.

The **Schema Update** page reappears, displaying the .tgz filename in the **Browse** field.

4. Click **Upload**.

Do not move away from the **Schema Update** page while the tgz file is uploading to Junos Space Network Management Platform. Note that the process can take some time, depending on how many schemas are in the file.

5. Select the desired schema and click **Install**.

The **Manage DMI Schemas** inventory landing page reappears, displaying the newly installed schema.

If you need to download the file from the SVN Repository, and you have not yet configured the connection to the repository:

1. Have the following to hand:

- URL : <https://xml.juniper.net/dmi/repository/trunk>
- Username: userName
- Password: userPasswd

2. Select the **SVN Repository** option button.

3. Click **Configure**.

The **SVN Access Configuration** dialog box appears.

4. Enter the SVN URL, the username and the password in the appropriate text fields. Click **Test Connection**.

A message appears to tell you whether the connection was established successfully or not.

5. Whether or not connection was successful, click **OK**.

The **SVN Access Configuration** dialog box reappears.

6. Either:

- If the connection failed, click **Cancel** , find the correct credentials, and repeat the above steps.
- If the connection was successful, click **Save**.

The **Schema Update** page reappears, displaying the SVN Repository URL.

If you need to install the file from the SVN Repository, and you have already configured the connection to the repository:

1. Select the SVN Repository option button.
2. Ensure the repository's URL appears in the URL field. If the field is blank, you must configure the connection. See step 3 above.
3. Click **Connect**.

The content of the repository with DMI schema releases appears in table form under **Available Updates** on the **Schema Update** page. The already installed versions are preselected.

Junos Space Network Management Platform detects and marks any missing schemas with a red arrow symbol. Missing schemas are the OS versions on devices that Junos Space Network Management Platform discovers in your network, but which have not been installed on Junos Space Network Management Platform.

You can sort by clicking on the column headings: Device Family, Release, Date. To change the display, click the arrow that appears when you click a column heading. To determine whether sorting should be ascending or descending, click the arrow that appears when you click a column heading.

4. (Optional) To display the recommended schemas only, select the **Show recommended schemas** check box.

Select the desired schemas.



NOTE: You need at least one schema for each device family in your network. See [“Setting a Default DMI Schema” on page 722](#).

Click **Install**.

A message appears, asking you to wait. After installation, the **Manage DMI Schemas** page reappears, displaying the new schema(s).

**Related
Documentation**

- [Managing DMI Schemas Overview on page 714](#)
- [Setting a Default DMI Schema on page 722](#)
- [Troubleshooting DMI Schema Management on page 723](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 719](#)

Creating a Compressed Tar File for Updating DMI Schema

This topic contains instructions for creating a compressed tar file (extension **.tgz** or **.tar.gz**) on Linux or Microsoft Windows. You use the compressed tar file to update a DMI schema on Junos Space Network Management Platform (see [“Updating a DMI Schema” on page 716](#))



NOTE: For both Linux and Microsoft Windows, ensure the following:

- The internal directory structure of the compressed tar file complies with the following format; that is, when you extract the compressed tar file, all files must be extracted to a folder structured as follows:
dmi/deviceFamily/releases/osVersion/...
- The compressed tar file has the **.tgz** or **.tar.gz** extension.
- You have the username and password for **xml.juniper.net**, which are your Juniper Networks support credentials.

To create a compressed tar file for updating DMI schema:



NOTE: In this topic, we provide examples that contain only HTTPS URLs. However, both HTTP and HTTPS URLs are supported. If the repository (whose URL is being entered) supports both HTTP and HTTPS access, we recommend that you use an HTTPS URL.

- On Linux, perform the following steps:



NOTE: The commands in this topic have been tested on CentOS and RedHat (Fedora). On other Linux distributions, use equivalent commands.

1. Install the Subversion (SVN) client on Linux. To install Subversion client on Linux, refer to [Install SVN on Linux](#) or other relevant documentation.
2. Create a temporary directory.
3. Navigate to the temporary directory created in the preceding step.
4. Check out the files from Subversion by executing the following command:

```
svn --username=userName --password=userPwd co dmiRepositoryURL
```

where *userName* and *userPwd* are the username and password required to access **xml.juniper.net**, and **dmiRepositoryURL** is the URL of the repository folder that you want to checkout.

Examples of the DMI repository URLs are shown in [Table 103 on page 720](#).

Table 103: Sample URLs for the Repository

Type	Example URL
For the whole Junos OS family	https://xml.juniper.net/dmi/repository/trunk/junos
For a device family	https://xml.juniper.net/dmi/repository/trunk/junos-es/
For a selected OS version	https://xml.juniper.net/dmi/repository/trunk/junos-ex/releases/11.2R2.4/

5. Tar the **dmi** directory by executing the following command from within the directory containing the **dmi** directory:

```
tar czvf filename dmi
```

where *filename* is the same of the compressed tar file. You can use any filename as long as the extension of the file is **.tgz** or **.tar.gz**

The compressed tar file is now ready for uploading into Junos Space Network Management Platform.

- On Microsoft Windows, perform the following steps:
 1. Install the Subversion (SVN) client on Microsoft Windows from the following location: [Install TortoiseSVN on Windows](#)



NOTE: To install the Subversion client, you can also use any software or tool that is equivalent to TortoiseSVN.

2. Install 7-Zip to generate a compressed tar file on Microsoft Windows by using the following link: [Install 7-Zip](#)



NOTE: To generate the compressed tar file, you can also use any software or tool that is equivalent to 7-Zip.

3. Create a temporary folder.



NOTE: You can use any name for the temporary folder.

4. Create a folder called **dmi** within the previously created temporary folder.
5. Right-click the **dmi** folder and select **SVN Checkout**:
A dialog box is displayed.

6. In the **URL of repository** field, enter the full URL of the repository. Refer to [Table 103 on page 720](#) for examples of URLs that you can enter.
7. In the **Checkout directory** field, enter the full path of the checkout directory; for example, `C:\test\dm\junos-es\`.



NOTE: The portion of the path to the right of the `dm` folder must be equivalent to the corresponding portion after `trunk` in the URL of the repository. For example, if the repository URL is <https://xml.juniper.net/dm/repository/trunk/junos-es/> the checkout directory path is `C:\test\dm\junos-es\`, and if the repository URL is <https://xml.juniper.net/dm/repository/trunk/junos-es/releases/10.1R3/>, the checkout directory path is `C:\test\dm\junos-es\releases\10.1R3\`.

8. In the **Checkout depth** field, enter **Fully recursive**.
9. Ensure that the **Omit externals** check box is cleared.
10. Select **HEAD revision**.
11. Click **OK**, and if you are prompted to, provide credentials.

The files are checked out from the Subversion repository into the specified folder.

12. Create the tar file from the **dm** folder using 7-Zip:
 - a. Right-click the **dm** folder and select **7-Zip**.
 - b. Click **Add to Archive**.
 - c. In the **Archive Format** field, select **tar**.
 - d. Click **OK**
13. Compress the tar file file using 7-Zip:
 - a. Right-click the **dm.tar** file and select **7-Zip**.
 - b. Click **Add to Archive**.
 - c. In the **Archive Format** field, select **gzip**.
 - d. Click **OK**
14. (Optional) Rename the ***.tar.gz** file to ***.tgz**

The compressed tar file is now ready for uploading into Junos Space Network Management Platform.

Related Documentation

- [Managing DMI Schemas Overview on page 714](#)
- [Setting a Default DMI Schema on page 722](#)
- [Updating a DMI Schema on page 716](#)

- [Troubleshooting DMI Schema Management on page 723](#)

Setting a Default DMI Schema

Set a default DMI schema for each device family to enable Junos Space Network Management Platform to apply an appropriate schema to a device family. In a clean install situation, Junos Space Network Management Platform automatically matches DMI schemas to device families, but in all other situations, you should set a default DMI schema for each device family.

When creating a device template definition, the system will use a default DMI schema for the device family unless you select a schema.

The configuration edit action in the Devices workspace always checks for an exact match between device and DMI schema. If it does not find a match, it will use the default schema (see [“Modifying Device Configuration Overview” on page 53](#)).

To set a default DMI schema:

1. Select **Administration > DMI Schemas**.

The **DMI Schemas** page appears, in the tabular view displaying the data in a table with the following columns:

- Device Family
- OS Version
- Device Series
- State—Whether default or not. An empty cell in this column means that the DMI schema in that row is not the default.

2. Select the row that contains the appropriate combination of device family, OS version, and device series, and from the Actions menu select **Set Default Schema**.

The **Set Default DMI Schema** dialog box opens, displaying the DMI schema name, device family, and OS version.

3. Click **Set Default**.

If any other schema was previously the default, in the tabular view, its cell in the **State** column empties, and the word “Default” appears in the State column for the selected schema.

4. (Optional) To remove the default status from a DMI schema, set another schema of the same family as the default.

Related Documentation

- [Managing DMI Schemas Overview on page 714](#)
- [Updating a DMI Schema on page 716](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 719](#)
- [Troubleshooting DMI Schema Management on page 723](#)

Troubleshooting DMI Schema Management

This topic describes common problems associated with DMI schema management and provides solutions where possible. The following are issues that might be encountered:

- No schemas in new installation of Junos Space Network Management Platform
- Schema tree not displayed

No schemas in new installation of Junos Space

When the Junos Space server first comes up, all the schemas for all the discovered devices should be pre-installed. Select **Administration > DMI Schemas**. There should be at least one schema per device family, and each device family should have one schema marked as default.

If the **DMI Schemas** page is empty, installation was unsuccessful.

There is no workaround for this problem.

Schema tree not displayed

Typically, if a schema is defective, its schema tree will not be displayed.

Verify that a particular schema has been parsed successfully: navigate to **Device Templates > Definitions > Create Template Definition** task. Select the schema in question and click **Next**.

The schema tree or hierarchy of configuration options should be displayed on the left. All nodes should be navigable, that is, it should be possible to drill down into the hierarchy to reach all the options.

If the topmost node (**Configuration**) cannot be opened to reveal the hierarchy, the schema was corrupted during porting (grep for SchemaMgr ERROR in server.log).



NOTE: One defective schema will not affect the other DMI schemas, which will still be available for use.

The solution to this problem is to replace one or more existing DMI schemas on the Junos Space server.

There are two ways of doing this:

- Using a script supplied by Juniper support. This requires restarting jboss.
- Using your own tgz file. This does not require restarting jboss.

For instructions, see [“Creating a Compressed Tar File for Updating DMI Schema” on page 719](#).

**Related
Documentation**

- [Managing DMI Schemas Overview on page 714](#)
- [Updating a DMI Schema on page 716](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 719](#)
- [Setting a Default DMI Schema on page 722](#)

CHAPTER 72

Generate Key

- [Key-based Authentication Overview on page 725](#)
- [Generating and Uploading Authentication Keys to Devices on page 726](#)

Key-based Authentication Overview

Junos Space Network Management Platform can discover and manage a device either by presenting credentials (username and password) or by key-based authentication.

Junos Space Network Management Platform supports RSA keys for key-based authentication. RSA is an asymmetric-key or public-key algorithm using two keys that are mathematically related. Junos Space Network Management Platform includes a default set of public-private key pairs. However, we recommend that you generate your own public/private key pair with a passphrase applied. Generate your keys by following the instructions in [“Generating and Uploading Authentication Keys to Devices” on page 112](#). The public key can be uploaded to devices being managed by Junos Space Network Management Platform. The private key is encrypted and stored on the system running Junos Space Network Management Platform. Junos Space Network Management Platform uses username and password credentials to log in to a device for the first time in order to copy and upload the public key. Any further communication to the devices is done using key-based authentication, without passwords.

It is advisable to protect the private key on the Junos Space system by using a passphrase, which is merely a long password that can include spaces and tabs and is much more difficult to break by brute-force guessing than is one shorter string.

You do not have to use RSA-based authentication on every device in your network; you can use passwords on some systems if you prefer or they require it.

Setting up key-based authentication between two computers is a multi-step process that is well described on many IT-related Internet sites (as is the public-key cryptography to which it is related). Junos Space Network Management Platform automates all of this key-creation and uploading process for you. It also tracks and reports the authentication status of each device in the Devices workspace.

Related Documentation

- [Generating and Uploading Authentication Keys to Devices on page 112](#)

Generating and Uploading Authentication Keys to Devices

- [Generating Keys on page 726](#)
- [Uploading Keys to Devices for the First Time on page 726](#)
- [Upload Keys on Managed Devices that have Conflicting keys with Junos Space on page 728](#)
- [Verifying Device Key Status on page 729](#)

Generating Keys

To generate a public/private key pair for authentication during login to network devices:

1. Select **Administration > Fabric** and select the Generate Key icon on the Actions menu. The Key Generator dialog box appears.
2. (Optional) In the **Passphrase** box, enter a passphrase to be used to protect the private key, which will remain on the system running Junos Space Network Management Platform and will be used during device logins.
The passphrase must have a minimum of 5 and a maximum of 255 characters. It may include spaces and tabs. A long passphrase with space and tab characters is harder to break by brute-force guessing. Although a passphrase is not required, it is recommended because it will impede an attacker who gains control of your system and tries to log in to managed network devices.
3. (Optional) Schedule the Junos Space Network Management Platform to generate the keys at a later time.
 - To specify a later start date and time for the key generation, select the **Schedule at a later time** check box.
 - To initiate the key generation as soon as you click **Generate**, clear the **Schedule at a later time** check box (the default).



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

4. Perform one of the following:
 - To generate the keys, click **Generate**.
 - To exit the Key Generator dialog box, click **Cancel**. The keys are not generated.

Uploading Keys to Devices for the First Time

To upload authentication keys to multiple managed devices for the first time:

1. Select **Devices > Device Management**.
The Device Management inventory page appears.
2. On the menu bar, click the **Upload Keys to Devices** icon.

The Upload Keys to Devices dialog box appears.

3. To upload keys to a single device:

a. Select **Add Manually**.

The Authentication Details box appears within the Upload Keys to Devices dialog box.

b. Select **IP Address** or **Hostname**.

c. In the **IP Address/Host Name** box, enter the IP address or the hostname of the target managed device.

d. In the **Device Admin** box, enter the appropriate username for that device.

e. In the **Password** box, enter the password for that device.

f. (Optional) To authorize a different user on the target device, select the **Authorize different user on device** check box and enter the username in the **User on Device** field.

If the username you specify in the **User on Device** field does not exist on the device, a user with this username is created and the key is uploaded for this user. If the **User on Device** field is not specified, then the key is uploaded for the "admin" user on the device.

g. Click **Next**.

h. Click **Finish** to upload keys to the device.

The Job Information dialog box appears.

i. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device. The Job Management page appears. View the job details to know whether this job is successful.

4. To upload keys to multiple devices:

a. Select **Import From CSV**.

b. (Optional) To see a sample CSV file as a pattern for setting up your own, select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

You should enter the device name, IP address, device password, and a username on the device. If the username you specify in the user on device column does not exist on the device, a user with this username is created and the key is uploaded for this user. If the user on device column is not specified, then the key is uploaded for "user admin" user on the device.

c. Once you have a CSV file listing the managed devices and their data, select **Select a CSV To Upload**. The Select CSV File dialog box appears.

d. Click **Browse** to navigate to where the CSV file is located on the local file system. Make sure that you select a file that has .csv extension.

e. Click **Upload** to upload keys to the device.

Junos Space Network Management Platform displays the following error if you try to upload non-csv file formats:

Please select a valid CSV file with '.csv' extension.

- f. Click **OK** on the information dialog box that appears. This dialog box displays information about the total number of records that were uploaded and whether this operation was a success.

You can see a green tick mark adjacent to the **Select a CSV To Upload** field, which indicates that the file has been successfully uploaded.

- g. Click **Next**.

- h. Click **Finish**.

The Job Information dialog box appears.

- i. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device. The Job Management page appears. View the job details to know whether this job is successful.

RSA Keys are uploaded automatically to all the managed devices (that were discovered through RSA authentication) in Junos Space, if a new key is generated on Junos Space.

Upload Keys on Managed Devices that have Conflicting keys with Junos Space

To upload authentication keys to one or several managed devices manually:

1. Select **Devices > Device Management**.
The Device Management inventory page appears.
2. Select the check boxes to the left of the names of the devices to which you want to upload keys.
3. On the menu bar, click the **Upload Keys to Devices** icon.
The IP address of the devices are pre-populated.
4. In the **User Name** field, enter the appropriate username for that device.
5. In the **Password** field, enter the password for that device. Confirm it by reentering it in the **Re-enter Password** box.
6. Select **Next** to provide details for the next device.
7. Select **Upload** to upload keys to the managed devices.
The Upload Authentication Key dialog displays a list of the devices with their credentials for your verification.



NOTE: If you do not specify a username in the User Name field, the key is uploaded for “user admin” user on the device. If the username you specify in the User Name field does not exist on the device, a user with this username is created and the key is uploaded for this user.

Verifying Device Key Status

To verify the authentication status of managed devices:

- Select **Devices > Device Management**.

The Device Management inventory page appears.

The Authentication Status column displays one of the following values:

- **Key Based**—Authentication key was successfully uploaded.
- **Credentials Based**—Key upload was not attempted; login to this device is by credentials.
- **Key Conflict**—Junos Space and device do not have the same key.
- **NA**—"NA" is displayed mostly for LSYS devices and wwJunos devices.

Related Documentation

- [Key-Based Authentication Overview on page 111](#)
- [Device Discovery Overview on page 131](#)
- [Discovering Devices on page 132](#)
- [Resolving Key Conflicts on page 116](#)

PART 13

Systems of Record and Disaster Recovery

- [Systems of Record and Disaster Recovery on page 733](#)

CHAPTER 73

Systems of Record and Disaster Recovery

- [Understanding Systems of Record in Junos Space on page 733](#)
- [Understanding Disaster Recovery on page 734](#)
- [Creating the DR Master Cluster on page 736](#)
- [Creating the DR Slave Cluster on page 739](#)
- [Performing a Reverse Restore on page 744](#)

Understanding Systems of Record in Junos Space

Although by default the Junos Space network you are administering is the system of record (SOR)--each device defines its own official state--you may prefer to have the Junos Space Network Management Platform database contain the official state of the network, enabling you to restore that official state if unwanted out-of-band changes are made to a device. This feature enables you to designate Junos Space Network Management Platform as the SOR if you prefer.

- [Systems of Record on page 733](#)
- [Implications on page 734](#)

Systems of Record

A network managed by Junos Space Network Management Platform has two repositories of information about the devices in it: the devices themselves (each device knows what is on it and can report that state), and the Junos Space Network Management Platform database (containing information reported during device discovery). One of these repositories must have precedence over the other as the accepted desirable state. By default, the network itself is the system of record (NSOR).

In NSOR, when a local user commits a change in the configuration of a network device, the commit triggers a report via system log to Junos Space Network Management Platform. The values in the Junos Space Network Management Platform database are automatically changed to match the new device values, and the timestamps are synchronized. Thus the devices control what is in the database.

As of version 12.2, you can designate the Junos Space Network Management Platform database values as having precedence over any values configured locally at a device. In this scenario, Junos Space Network Management Platform (database) is the system of record (SSOR). It contains the configurations that the Junos Space administrator considers

best for the network devices. If an out-of-band commit is made on a network device, Junos Space Network Management Platform receives a system log message, but the values in the Junos Space Network Management Platform database are not automatically changed or synchronized. Instead, the administrator can choose whether or not to overwrite the device's local changes by pushing the accepted configuration to it from the Junos Space Network Management Platform database.

The choice of pushing the Junos Space Network Management Platform configuration is left to the administrator because the local device changes may, for example, be part of a temporary test that the administrator would not want to interrupt. Should the tester forget to reset the configuration at the end of the test, however, the administrator might then push the SSOR configuration to the device.

Implications

The basic difference between NSOR and SSOR lies in whether or not the Junos Space Network Management Platform database is automatically synchronized when changes are made in a network device, and which set of values has precedence.

Setting the Junos Space Network Management Platform database as the system of record does not protect your network from local changes. It does notify Junos Space Network Management Platform via system log when they occur, and it does not resynchronize, so you still have the previous configuration and you can reset the remote device quickly if you need to do so. Under an NSOR scenario, Junos Space Network Management Platform is also notified via system log. You can still push a more desirable configuration to the device, but the process is less efficient.

In the NSOR scenario, you can disable automatic resynchronization. When auto-resync is turned off, the server continues to receive notifications and goes into the out-of-sync state; however, the auto-resync does not run on the device. You can manually resynchronize a device in such a case.

NSOR with automatic resynchronization disabled is not equivalent to SSOR: manually resynchronizing under NSOR updates the values in the Junos Space Network Management Platform database to reflect those on the device. This never happens under SSOR, where the Junos Space Network Management Platform database values have precedence over the device values, and synchronizing them involves pushing the database values to the device, effectively resetting its out-of-band changes.

- Related Documentation**
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 47](#)

Understanding Disaster Recovery

- [Overview on page 735](#)
- [Prerequisites on page 735](#)

Overview

Junos Space provides a means to recover from disaster, by enabling mirroring of the original Junos Space installation on a cluster of nodes at a geographically remote location. If the main Junos Space site failed due to a disaster such as an earthquake, the other site would take over.

The physical installation is a set of two geographically separate clusters, the DR Master cluster (the main site) and the backup or DR Slave cluster (the remote site). Backups contain:

- Junos Space Network Management Platform and other application databases
- Firewall rules
- SNMP configuration of Junos Space
- Device schema information
- Network monitoring database information
- Real-time performance monitoring information

The disaster recovery (DR) system is entirely driven by back-end scripts. Currently, these scripts must be configured manually.

You perform the following sequence of operations to set a disaster recovery system:

1. Back up the DR Master cluster to the DR Slave cluster. See [“Creating the DR Master Cluster” on page 736](#).
2. If disaster overtakes the original DR Master, stop the DR Slave from pulling the backups from the DR Master. See [“Creating the DR Slave Cluster” on page 739](#).
3. When your original DR Master comes back online, perform a reverse restore to make it a DR Slave. See [“Performing a Reverse Restore” on page 744](#).

Prerequisites

The requirements for recovering your Junos Space installation from a disaster are as follows:

- The DR Master cluster at the primary site (which can be a single node or multiple nodes) and the DR Slave cluster at the remote site (a single node or multiple nodes) must be set up in exactly the same way, with all the same applications, device adapters, and so on.
- When a new node is added to the cluster, the backup and restore scripts must be rerun to update the configuration.
- Both clusters should be configured through the graphical user interface (GUI) with SMTP server information (see [“Managing SMTP Servers” on page 683](#)). This configuration enables both the DR Master and the DR Slave clusters to notify you by e-mail if the replications fail.



NOTE: We recommend that the e-mail server information be the same on both the DR Master and the DR Slave clusters to avoid the following situation:

If the DR Master is configured with e-mail server 1 and the DR Slave is configured with e-mail server 2, when restoring the database, e-mail server 2 is removed, and only e-mail server 1 remains.

- Both ICMP and SCP must be enabled between the DR Master and DR Slave clusters.
 - Backup and restore cannot be done on the same server.
 - Backup configuration and Restore configuration should be done only on the VIP node of respective clusters. If a VIP switchover occurs, you need to rerun backup or restore (depending on the role) on the new VIP node.
 - ScreenOS devices, which are added to Junos Space using the Add Deployed Devices task, need to be rediscovered after disaster recovery. You have two options for reconnecting back to a ScreenOS device, either
 - Use Junos Space to delete the device and rediscover it.
- or
- Change the IP address of the device to point to the DR Slave cluster in the nsmgmt section.

After you perform one of the options, the device reconnects.

Related Documentation

- [Creating the DR Master Cluster on page 736](#)
- [Creating the DR Slave Cluster on page 739](#)
- [Performing a Reverse Restore on page 744](#)

Creating the DR Master Cluster

To set up the main cluster, the DR Master cluster, run three scripts as described in the following sections:

Backup configuration and Restore configuration should be done only on the VIP node of the Master cluster. If a VIP switchover occurs, you must rerun the backup script on the new VIP node.

The role change from DR Slave to DR Master (backup to restore) and vice versa cannot be made directly. It can only be made after the initial role is stopped.

The scripts used are located here: `/opt/jmp-geo/backup/script/backup.sh – script`



NOTE: When a new node is added to the cluster, the backup and restore scripts must be rerun to update the configuration.



NOTE: After you run the restore script, the network monitoring node list might contain previous Space Servers as well.

- 1. [Configuring the DR Master Cluster on page 737](#)
- 2. [Starting the Backup for the DR Master Cluster on page 738](#)
- 3. [Stopping the Backup on page 739](#)

1. Configuring the DR Master Cluster

Configuring the DR Master cluster enables you to input the following information which is then stored in the **backup.properties** file:

- The e-mail address for notifications
- The DR Slave VIP IP address
- The DR Slave device management IP addresses
- The number of backup files to be kept
- The time at which the backup should be run
- The number of days per week the backup should run

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./backup.sh config
```

Please enter contact email address in case of Disaster Recovery Slave failure:

```
user1@example.com
```

Backup configurations...

Creating /etc/ssmtp/ssmtp.conf...

Creating /etc/ssmtp/revaliases...

Please enter DR Slave Cluster management ip(VIP) :

```
10.10.10.10
```

Please enter DR Slave Cluster device management ip(comma separated) :

```
10.10.10.63,10.10.10.65
```

```
checking ip: 10.10.10.63
```

```
checking ip: 10.10.10.65
```

Please enter max backup files to keep(default=3):

Notice: cron job takes format of digits joined by ',', For every instance enter '*'

Please enter hours of the day to run backup:

0

Please enter days of the week to run backup, Sun= 0, Sat=6:

6



NOTE: You should enter the hours of the day to run backup in a 24-hour format.

2. Starting the Backup for the DR Master Cluster

Starting the backup for the DR Master cluster causes a recurring job to be put in the cron. It can be viewed using **crontab -l**.

The backups are stored in the same server in **/opt/jmp-geo/backup/data** in TGZ. Verify the status of the backup process in **/opt/jmp-geo/backup/backup.log**. If the DR Slave is not available, you are notified by e-mail, as configured in the previous section.

If the device discovery mode is DIC, the script also adds the outbound-SSH of the DR Slave cluster's device management IP address to the Junos Space-managed devices.

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./backup.sh start
```

```
Demoting this cluster from the DR Master Cluster Role ...
```

```
update cluster state successful
```

```
Stopping backup cron job...
```

```
Stopping crond: [ OK ]
```

```
Starting crond: [ OK ]
```

```
Promoting this cluster to the DR Master Cluster Role ...
```

```
update cluster state successful
```

```
Adding DR Slave Cluster device management ip to devices ...
```

```
save cluster ip successful
```

```
save cluster ip successful
```

```
queue http://10.0.0.1:8080/api/hornet-q/queues/jms.queue.jmpgeoq4327 creation  
successful
```

```
update-devices-with-ip 10.10.10.65 successful
```

```
delete http://10.0.0.1:8080/api/hornet-q/queues/jms.queue.jmpgeoq4327 successful
```

Starting backup cron job...

Stopping crond: [OK]

Starting crond:

The DR cron job is started on the DR master.

3. Stopping the Backup

Do not transition from DR Master to DR Slave directly. Stop the initial role first. Choose one of the following methods of transitioning:

- Promote a normal cluster to DR Master
- Demote a normal cluster to DR Slave
- Disable a DR Master so that it becomes a normal cluster
- Disable a DR Slave so that it becomes a normal cluster

Stopping the backup removes the cron job and stops the backup being performed.

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./
```

```
backup.sh stop
```

```
Demoting this cluster from the DR Master Cluster Role ...
```

```
update cluster state successful
```

```
Stopping backup cron job...
```

```
Stopping crond: [ OK ]
```

```
Starting crond: [ OK ]
```

```
[user1@host script]#
```

Related Documentation

- [Understanding Disaster Recovery on page 734](#)
- [Creating the DR Slave Cluster on page 739](#)
- [Performing a Reverse Restore on page 744](#)

Creating the DR Slave Cluster

The DR Slave cluster takes over when disaster has overtaken the DR Master cluster. The `/opt/jmp-geo/restore/script/restore.sh` script uses SCP to pull the backups from the DR Master cluster and when required, restore the DR Slave with the information from the DR Master.

The following four operations involved in setting up the DR Slave cluster:

Backup configuration and Restore configuration should be done only on the VIP node of the DR Master cluster or the DR Slave cluster. If a VIP switchover occurs, you must rerun the backup or restore script (depending on the role) on the new VIP node.



NOTE: When a new node is added to the cluster, the backup and restore scripts must be rerun to update the configuration.



NOTE: After you run the restore script, the network monitoring node list might contain previous Junos Space Servers as well.

The role change from Slave to Master (backup to restore) and vice versa cannot be made directly. It can only be made after the initial role is stopped.

The scripts used for this purpose are located here: `/opt/jmp-geo/restore/script/restore.sh – script`.

- [1. Configuring the DR Slave Cluster on page 740](#)
- [2. Starting to Pull the Backups From the DR Master on page 741](#)
- [3. Stopping Pulling the Backups from the DR Master on page 742](#)
- [4. Restoring on page 743](#)

1. Configuring the DR Slave Cluster

Configuring the DR Slave cluster records the following information in the `restore.properties` file:

1. The e-mail address to receive notifications
2. The DR Master VIP address
3. The DR Master passwords, if there are multiple nodes
4. The SCP timeout
5. The time at which the backups are to be pulled from the DR Master
6. The number of days per week the backups are to be pulled from the DR Master

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./
```

```
restore.sh config
```

```
Please enter contact email address in case DR Master failure:
```

```
user1@example.com
```

```
Backup configurations...
```

```
Creating /etc/ssmtp/ssmtp.conf...
```

Creating /etc/ssmtp/revaliaes...

Please enter DR Master Cluster management ip(VIP) :

10.10.10.10

Please enter DR Master Cluster VIP node admin passwords(comma separated):

abc123

Please enter scp timeout in seconds:

120

Notice: cron job takes format of digits joined by ',', For every instance enter '*' Please enter hours of the day to pull backup files:

0

Please enter days of the week to pull backup files, Sun= 0, Sat=6:

0

Testing SCP from DR Master to DR Slave...

2. Starting to Pull the Backups From the DR Master

The script shown in this section starts pulling the backups from the DR Master cluster.

It creates a cron job entry, which can be viewed by using **crontab -l**.

If the DR Master is not available, you receive the e-mail notification you configured in the previous section.

The copied files are located in the **/opt/jmp-geo/restore/data** folder. The restore polling status is located in the **/opt/jmp-geo/restore/restore.log**.

At this point, the script blocks all connections to devices, since this is a slave cluster (that is, no devices can be discovered).

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./
```

```
restore.sh startPoll
```

```
Enabling this cluster to the DR Slave Cluster Role ...
```

```
update cluster state successful
```

```
blocking port 7804 on space-005056b206b7....
```

```
reloading firewall...
```

```
Starting jmp-firewall: [ OK ]
```

```
finish reloading

<response>

<message>

</message>

<status>SUCCESS</status>

</response>

Starting restore cron job...

Stopping crond: [ OK ]

Starting crond: [ OK ]
```

3. Stopping Pulling the Backups from the DR Master

The script in this section stops pulling the backups from the DR Master, and thereby demotes the cluster from the DR Slave cluster role and removes the cron job entry.

Do not transition from DR Master to DR Slave directly. Stop the initial role first. Choose one of the following methods of transitioning:

- Promote a normal cluster to DR Master
- Demote a normal cluster to DR Slave
- Disable a DR Master so that it becomes a normal cluster
- Disable a DR Slave so that it becomes a normal cluster

Stopping the backup removes the cron job and stops the backup being performed.

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./
restore.sh stopPoll

Stopping restore cron job...

Stopping crond: [ OK ]

Starting crond: [ OK ]

Demoting this cluster from the DR Slave Cluster Role ...

update cluster state successful

opening port 7804 on space-005056b206b7....

jmp-firewall is stopped. Skip reloading

<response>
```

```
<message
</message>

<status>SUCCESS</status>

</response>
```

4. Restoring

Running the restore script enables the DR Slave to take over the management role when disaster overtakes the DR Master. The script carries out the following four operations:

1. Stops JBoss and the network monitoring service, inflates the files from the latest backup that was pulled, and brings the whole system back up.
2. Enables all connections to the devices.



NOTE: You cannot run the restore script when the DR Master is present and online. This procedure is for disaster recovery scenarios only.

3. If the devices were originally discovered using DIC mode, reconfigures Junos Space-managed devices to point to the DR Slave cluster so that devices connect back to the DR Slave cluster.
4. Reconfigures all the devices to point the SNMP trap group to the DR Slave cluster, so that traps and alarms are received by the DR Slave cluster.

Run the script as follows. The output shown reflects the sample input.

```
[user1@host script]# ./
```

```
restore.sh restore
```

The DR Master is down, restore procedure continues.

The latest backup files is : /opt/jmp-geo/restore/data/825763000.tgz

Do you want to continue (yes/no):

```
yes
```

Disaster Recover Procedure: The DR Master Cluster must be down,
turning this DR Slave Cluster to be in service ...

```
update cluster state successful
```

```
opening port 7804 on user1@host....
```

```
reloading firewall...
```

```
Starting jmp-firewall: [ OK ]
```

finish reloading

<response>

<message>

</message>

<status>SUCCESS</status>

</response>

Extracting backup files....

Set node into restore state

**Related
Documentation**

- [Understanding Disaster Recovery on page 734](#)
- [Creating the DR Master Cluster on page 736](#)
- [Performing a Reverse Restore on page 744](#)

Performing a Reverse Restore

You perform a reverse restore to reestablish a disaster recovery system by creating a new DR Slave at a site geographically separate from the site where your new DR Master is located. For example, if your original DR Master was in Chicago, and your DR Slave was in London, if the London site is overtaken by a further disaster, you would get your original site, Chicago, back online, and then create a DR Slave in Chicago because London would be the new DR Master.

This topic provides instructions for performing a reverse restore.

1. Configure your new DR Master (in the example above, the London site) for backup. See [“Creating the DR Master Cluster” on page 736](#).
2. At the new DR Slave site, reinstall the same version of Junos Space with the same IP addresses, applications and adapters used originally (in the example above, Chicago). See the Prerequisites section of [“Understanding Disaster Recovery” on page 734](#).
3. Configure the new DR Slave site for restore. See [“Creating the DR Slave Cluster” on page 739](#).



NOTE: After you run the restore script, the network monitoring node list might contain previous Junos Space Servers as well.

**Related
Documentation**

- [Understanding Disaster Recovery on page 734](#)
- [Creating the DR Master Cluster on page 736](#)
- [Creating the DR Slave Cluster on page 739](#)

PART 14

Index

- [Index on page 747](#)

Index

Symbols

#, comments in configuration statements.....	xxxiii
(), in syntax descriptions.....	xxxiii
< >, in syntax descriptions.....	xxxiii
[], in configuration statements.....	xxxiii
{ }, in configuration statements.....	xxxiii
(pipe), in syntax descriptions.....	xxxiii

A

AAA	
configuring.....	673
access control	
object level.....	701
Add deployed devices	
overview.....	141
add devices	
overview.....	143
adding deployed devices.....	139
adding devices.....	145
adding Junos Space application.....	635
administration	
smtp server	
add	684
administrators	
CLI.....	547
maintenance mode.....	548
overview.....	547
user interface See user administration	
alarm notification	
configuration overview.....	435
configuring.....	438
alarms	
viewing and managing.....	119, 391
application	
adding.....	635
Platform, adding.....	641
uninstalling.....	646
upgrading.....	638
application dashboard.....	13

applications	
managing.....	621
settings, modifying.....	624
auto resync device.....	624
automatic logout of idle user sessions	
(mins).....	624
maximum auto resync waiting time	
(secs).....	624
assets	
tracking and searching for.....	377
assigned shared objects	
unassigning.....	68
viewing.....	68
attribute	
certificate.....	665
audit log	
UTC to local timestamp, converting.....	536
audit logs	
archive file, naming conventions.....	539
archiving and purging.....	539
archiving to local server.....	539
archiving to remote server.....	540
default directory.....	532
exporting.....	543
overview.....	531
table view.....	532
user privileges.....	532
viewing	
most active users in last 24 hours.....	536
statistics.....	534
audit logs table	
description.....	532
job ID.....	532
task results.....	532
timestamp.....	532
audit trails	
exporting.....	543
authentication and authorization	
configuring a RADIUS server for.....	673
configuring TACACS+ for.....	677
authentication mode.....	661
authentication modes	
local.....	668
remote.....	668
remote-local.....	668
authentication server	
creating.....	670
modifying.....	672
auto resync device application setting.....	624

automatic logout of idle user sessions (mins)	
application setting.....	624
automatic resynchronization	
disabling.....	49
B	
backup and restore See database	
braces, in configuration statements.....	xxxiii
brackets	
angle, in syntax descriptions.....	xxxiii
square, in configuration statements.....	xxxiii
C	
CA certificate.....	660
certificate	
attribute.....	665
errors.....	662
expiry.....	665
installing.....	662
managing.....	657
PKCS # 12 format.....	664
X.509 format.....	663
certificate revocation list (CRL).....	660
changing user passwords.....	4, 522
charts	
viewing.....	403
Checksum verification.....	286
checksum verification	
deleting results	336
procedure.....	302
verification result page controls	
description.....	336
viewing results	336
child	
subobject.....	704
CLI administrator	
changing password.....	547
name.....	547
tasks.....	547
commands	
show,	
using in Junos Space.....	96
comments, in configuration statements.....	xxxiii
commit script.....	275, 300
conditions for deleting a fabric node.....	567
configuration change log	
viewing.....	66
configuration file	
editing.....	450
configuration file editing	
, selecting perspective.....	54
configuration file inventory	
viewing.....	446
configuration file management	
overview.....	444
user privileges in.....	445
configuration files	
backing up.....	454
comparing.....	448
deleting.....	446
exporting.....	452
restoring.....	447
configuration filter	
adding.....	53
configuration options	
, editing.....	55
finding.....	199
configuration views	
managing.....	261
overview.....	255
user roles.....	257
variables.....	256
viewing statistics.....	263
workflow.....	256
configuring application setting.....	634
configuring application settings.....	626
connection status, for managed devices.....	43
consolidated config	
validating.....	60
consolidated configurations	
generating.....	59
conventions	
text and syntax.....	xxxii
CSV file	
uploading device network name and	
credentials via.....	132
CSV files, managing	
overview.....	204
curly braces, in configuration statements.....	xxxiii
customer support.....	xxxiv
contacting JTAC.....	xxxiv
D	
dashboard.....	13
data collection	
SNMP	
turning on and off.....	372

database		device discovery	
backup and restore, overview.....	604	authentication.....	131
device configuration data.....	132	Device Management Interface (DMI).....	131
device inventory data.....	132	inventory and configuration data.....	132
Database		overview.....	131
restoring from remote file.....	611	specifying a probe method.....	135
database backup		specifying credentials.....	136
default directory.....	605	specifying device targets.....	133
deleting files.....	614	viewing detailed reports.....	137
local.....	606	viewing status.....	137
overview.....	604	Device image deployment	
recurrence info, viewing.....	471, 615	in-service software upgrade.....	286
recurring job.....	605	Device Images	
remote host.....	608	Overview.....	273
viewing files.....	613	device images and scripts overview.....	269
database reports		device instances	
overview.....	368	deploying.....	149
sending.....	400	device inventory	
viewing.....	400	data.....	132
viewing pre-run reports.....	401	exporting.....	40, 86
database restore		overview.....	40
local.....	610	device job failure	
overview.....	605	retrying.....	472
default gateway, changing.....	561	device management	
definition		overview.....	35
exporting a.....	187	device management IP	
importing a.....	206	adding.....	561
definition states		deleting.....	561
template.....	182	device network name and credentials	
definitions, importing		uploading via CSV file.....	132
overview.....	205	device template	
Deleting a Device Image	293	creating.....	223, 227
deleting scripts		overview.....	222, 227
from devices.....	307	device template definitions	
from Junos Space.....	299	inventory viewing.....	185
deleting template definitions.....	187	device templates	
deleting user.....	522	deleting.....	212
deployed devices		deploying.....	213
managing.....	142	inventory viewing.....	225
Deploying a Device Image	286	modifying.....	214
device		overview.....	178, 209
troubleshooting.....	49	removing.....	215
device configuration		statistics viewing.....	181, 226
approving.....	57	undeploying.....	215
deploying.....	57	workflow.....	181
editing.....	53	devices	
rejecting.....	57	changing resync time delay.....	49
device configuration data.....	132	connecting to managed devices.....	106
device connection status.....	43	connecting to unmanaged devices.....	107, 108

connection status icons.....	44
deleting from Junos Space.....	93
disabling auto-resync.....	49
discovering.....	132
discovery, overview.....	131
exporting	
license inventory.....	80
software inventory.....	84
logical interfaces, viewing.....	77
logical inventory	132
management, overview.....	35
physical interfaces, viewing.....	76
physical inventory	132
removing provisioning services before deleting	
from Junos Space.....	94
resynchronizing managed devices.....	94
SSH connection.....	105
unmanaged, adding.....	153
using show commands in Junos Space.....	96
viewing	
connection status.....	41
hardware inventory.....	41
interfaces.....	41
IP address.....	41
license inventory.....	41, 80
operating system version.....	41
platform.....	41
software inventory.....	84
statistics, by connection status.....	37
statistics, by Junos OS release.....	38
statistics, by platform.....	37
viewing deployment details.....	70
disabling scripts.....	306
configuration example.....	306
disabling users.....	515
discovery See device discovery	
DMI Schema	
management overview.....	714
DMI schema	
troubleshooting.....	723
updating a.....	716
DMI schemas	
adding.....	719, 722
documentation	
comments on.....	xxxiii
downloading troubleshooting system log files	
using CLI.....	653
E	
enabling scripts.....	304
configuration example for a commit	
script.....	304
configuration example for an event	
script.....	304
configuration example for an op script.....	304
enabling users.....	515
error	
certificates.....	662
error messages	
SSH session.....	106
event script.....	275, 300
events	
viewing, querying, acknowledging.....	388
executing scripts.....	309
with JUISE.....	104
expiry	
certificate.....	665
exporting	
operation.....	320
exporting a	
definition.....	187
exporting scripts.....	337
F	
fabric	
adding a node.....	556
connection status.....	558
CPU resource.....	558
device connection IP address.....	558
disk space.....	559
load history.....	570
management IP address.....	558
memory resource.....	559
monitoring node status	
application logic.....	557
database.....	557
load balancer.....	557
node functions	
availability.....	555
multinode.....	553
single node.....	552
node name.....	558
node serial number.....	560
node threshold limit.....	553
overview.....	551, 556
self monitoring.....	570
system health.....	568

fabric node	
deleting.....	567
failed	
device, retrying a job on.....	472
font conventions.....	xxxii

G

generated reports	
viewing.....	360
getting started assistants, using.....	5
<i>See also</i> help, accessing	
global action icons.....	10
Help.....	10
Log Out.....	10
My Jobs.....	10
User Preferences.....	10
global search.....	20

H

hardware inventory	
viewing.....	73
Help icon.....	10
help, accessing.....	6, 10
<i>See also</i> getting started assistants, using	
hierarchical tags	
managing.....	689

I

icons	
help.....	10
job status.....	466
log out.....	10
my jobs.....	10
user preferences.....	10
image	
deploying a device.....	286
importing	
operation.....	322
importing a	
definition.....	206
importing definitions	
overview.....	205
importing scripts	
overview.....	313
procedure.....	313
in-service software upgrade.....	286
installing	
certificate.....	662

inventory page	
EOL data.....	75
objects, tagging.....	695
inventory pages	
filtering.....	27
ISSU.....	286

J

job status icons.....	466
jobs.....	466
archiving.....	473
canceling.....	470
management overview.....	461
purging.....	473
types.....	461
viewing	
scheduled jobs.....	466
your jobs.....	465
viewing statistics	
by execution time.....	470
by state.....	469
by type.....	469
JUISE.....	104
Junos OS release <i>See</i> devices categorized by	
Junos Space	
as system of record.....	733
device discovery.....	132
user account, creating.....	509
Junos Space license, managing.....	619
Junos Space software	
base application.....	640
hot-pluggable applications.....	640
network management platform,	
upgrading.....	641
upgrade highlights.....	640
upgrade scenarios.....	640
upgrading , before you begin.....	640

K

Key SNMP Customized (KSC) Performance reports	
creating.....	397
viewing.....	399
Key SNMP Customized (KSC) reports	
overview.....	368

L

license	
60-day trial.....	617
generating.....	617

Junos Space, managing.....	619
key file	
generating.....	618
uploading.....	618
license information.....	132
license inventory	
device	
viewing.....	41
exporting.....	80
viewing.....	80
Linux hardware	
SNMP monitoring.....	586
local authentication mode.....	668
local password	
for remote authentication, clearing.....	523
Log Out icon.....	10
logging in to Junos Space with remote	
authentication configured.....	679
logging in, to Junos Space.....	3
<i>See also</i> logging out, from Junos Space	
logging out from Junos Space.....	10
logging out, from Junos Space.....	6
<i>See also</i> logging in, from Junos Space	
logical interfaces	
viewing.....	77
login behavior	
remote authentication.....	365, 679
remote-local authentication.....	680
login credentials for manage devices	
changing.....	110

M

maintenance mode	
actions menu.....	549
administrator name.....	548
administrator password.....	548
administrator tasks.....	548
connecting to Junos Space appliance.....	549
lock time out.....	549
log in screen.....	548
overview.....	548
system locking.....	549
user administration.....	549
manage applications overview.....	621
Manage Applications workspace	
application, adding.....	635
application, uninstalling.....	646
application, upgrading.....	638
Platform, upgrading.....	641

Manage Scripts page	
fields description	276
management	
configuration file	
user privileges in.....	445
performance.....	365
management IP	
changing in same subnet.....	561
changing to different subnet.....	561
multinode	
changing in same subnet.....	561
managing applications.....	622
managing Junos Space license.....	619
managing template definitions.....	183
manuals	
comments on.....	xxxiii
maximum auto resync waiting time (secs)	
application setting.....	624
MD5 Validation Results	
Viewing	
Deleting.....	295
Modifying Device Image Details.....	294
modifying template definition.....	185
modifying users.....	520
monitoring	
fabric nodes.....	570
My Jobs feature.....	465
My Jobs icon.....	10

N

name and credentials	
device	
uploading via CSV file.....	132
network as system of record.....	733
network monitoring	
configuring.....	405, 407
dashboard, viewing.....	375
interfaces, managing.....	411
modifying users.....	405
reports	
overview.....	368
restarting.....	631
searching for nodes or asset information.....	374
services, managing.....	411
starting.....	631
stopping.....	631
viewing and tracking service outages.....	387

- viewing system configuration.....406
- workspace
 - overview.....365
 - remote authentication login
 - behavior.....365
- network monitoring services
 - restarting.....631
 - starting.....631
 - stopping.....631
- network name and credentials
 - device
 - uploading via CSV file.....132
- network settings
 - configuration guidelines.....561
 - configuring.....561
- network topology
 - adding nodes to a group.....384
 - creating a group for nodes.....383
 - filtering nodes.....381
 - managing alarms.....380
 - pinging nodes.....382
 - removing nodes from a group.....384
 - viewing alarms by node.....382
 - viewing alarms for nodes.....379
 - viewing events by node.....383
 - viewing network service details across
 - nodes.....385
 - viewing network services.....385
 - viewing node details.....381
 - viewing nodes.....379
 - viewing nodes with active alarms.....380
 - viewing resource graphs by node.....383
 - viewing topology map with different
 - layouts.....381
- networking monitoring
 - resyncing nodes.....372
- node
 - adding to fabric.....556
 - definition.....551
 - deleting.....567
 - threshold limit for devices.....553
- node functions
 - application logic.....553
 - database.....553
 - load balancer.....553
- node lists for performance management
 - viewing371
- nodes
 - resyncing372, 733
 - searching for.....374
- notification
 - status
 - configuring network monitoring.....407
- notifications
 - configuring.....416
 - destination paths, configuring.....418
 - event notifications, configuring.....416
 - path outages, configuring.....419
 - scheduled outages, configuring.....419
 - viewing and searching for.....395
- NSOR See network as system of record
- O**
 - object level access control.....701
 - object tagging
 - untagging.....697
 - viewing.....696
 - object, inventory
 - applied tags, managing688
 - filtering using tags.....697
 - tag, creating698
 - tags, managing.....687
 - op script.....275, 300
 - operations copying.....319
 - operations creating.....315
 - operations deleting.....320
 - operations exporting.....320
 - operations importing.....322
 - operations modifying.....317
 - operations overview.....279
 - operations running.....318
 - operations viewing.....339
 - options
 - configuration, finding.....199
 - outages See service outages
 - overview
 - definitions, importing.....205
 - importing definitions.....205
 - subobjects.....704
- P**
 - parent
 - subobject.....704
 - parentheses, in syntax descriptions.....xxxi
 - password, user, changing.....10
 - performance See system performance

performance management	
Admin, configuring network monitoring.....	405
notification status.....	407
alarms, viewing and managing.....	119, 391
assets, tracking and searching for.....	377
deleting reports.....	403
event viewing, querying, acknowledging.....	388
notifications, configuring.....	416
notifications, viewing and searching for.....	395
resyncing nodes.....	372
searching for nodes.....	374
surveillance categories, managing.....	433
thresholds, managing.....	411
viewing and tracking outages.....	387
viewing charts.....	403
viewing event details.....	390
viewing events.....	389
viewing node lists.....	371
viewing reports.....	398
Permission Labels	
assigning to users.....	706
attaching to objects.....	707
creating.....	706
deleting.....	706
managing.....	701
managing subobjects.....	709
removing from objects.....	707
removing from users.....	706
renaming.....	706
subobject.....	704
physical interfaces	
viewing.....	76
PKCS #12 format certificate.....	664
predefined role, managing.....	502
modifying.....	503
publishing template definition.....	184
R	
RADIUS authentication methods supported.....	667
RADIUS server	
configuring a	673
rebooting nodes.....	566
recurring database backup.....	605
remote authentication	
configuring servers.....	669
Junos Space login behavior.....	679
local password, clearing.....	523
method, selecting.....	669
overview.....	667
password, setting.....	510
server settings, modifying.....	672
server, creating.....	670
remote authentication mode.....	668
remote host	
database backup.....	608, 613
remote-local authentication mode.....	668
replacement device	
activating.....	102
report definition	
creating.....	355
managing.....	356
reports	
resource graphs	
viewing.....	399
restoring a database	
overview.....	605
resynchronization	
system of record and	733
Resynchronize with Network command.....	40
resynchronizing See devices	
RMA state	
putting a device in.....	101
role	
predefined, managing.....	502, 503
user-defined, deleting.....	507
user-defined, managing.....	502, 503, 505, 506
role-based administration.....	479
authentication.....	479
enforcement by workspace.....	480
overview.....	479
RBAC enforcement.....	479
RBAC enforcement, limitations.....	480
See also user administration	
roles See user administration	
predefined.....	481
Rules in device template definitions	
working with.....	203
S	
scheduled job statistics	
viewing.....	469
scheduled outages, configuring.....	419
schema	
updating a DMI.....	716
schema management	
troubleshooting DMI	723
schemas	
adding DMI.....	719, 722

- script details
 - Script Details Dialog Box Controls
 - Description.....335
- script modification.....297
- script types
 - modifying.....298
- script versions
 - comparing.....299
- scripts
 - overview.....275, 300
- search
 - global.....20
- Secure Console
 - connecting to devices.....106
 - overview.....105
 - terminal control characters.....108, 109
 - user privileges.....105
- Secure Copy (SCP) command
 - database backup.....605
- service outages
 - viewing and tracking.....387
- services, network monitoring
 - restarting.....631
 - starting.....631
 - stopping.....631
- show commands
 - using in Junos Space.....96
- SNMP community names, configuring.....410
- SNMP data collection
 - turning on and off.....372
- SNMP data collection, configuring.....410
- SNMP MIBs
 - clearing console logs.....422
 - compiling.....421
 - deleting.....421
 - uploading.....420
 - viewing.....421
- software inventory
 - exporting.....84
 - viewing.....84
- software upgrade
 - in-service.....286
- software, Junos Space, upgrading.....637, 639
- SOR See system of record
- specifying device-specific data in template
 - definitions.....200
- SRX device clusters
 - configuring.....157
- SSH session
 - connecting to managed devices.....106
 - connecting to unmanaged devices.....107, 108
 - error messages.....106
 - overview.....105
- SSoR
 - Space as System of Record.....626
- SSOR See Junos space as system of record
- Staging a Device Image284
- states
 - template definition.....182
- statistics
 - audit logs.....534
 - devices.....36
 - jobs.....469
 - users.....524
- statistics reports
 - generating for export.....402
 - viewing.....401
- status
 - notification
 - configuring network monitoring.....407
- subobject
 - Permission Labels.....704
- subobjects
 - child.....704
 - dependencies.....704
 - managing.....709
 - overview.....704
 - parent.....704
 - permission label.....709
- super administrator.....480
 - privileges.....480
 - See also user administration
- support, technical See technical support
- surveillance categories, managing.....433
- syntax conventions.....xxxii
- system
 - connecting to appliance in maintenance
 - mode.....549
 - database restore.....548
 - debugging.....548
 - performance
 - improving.....473
 - shutdown.....548
- system locking See maintenance mode
- system of record
 - networks as.....626
 - setting.....624

Space as.....	626
understanding.....	733
system status log file.....	647
checking, customize.....	649
downloading.....	648
downloading using SCP.....	654
downloading using USB device.....	653
files to download, customize.....	650
system status log file overview.....	647

T

TACACS+	
configuring.....	677
tagging managed objects.....	695
tags	
creating.....	695, 698
deleting.....	695
inventory objects, filtering.....	697
managing.....	687, 688
renaming.....	694
sharing.....	693
untagging.....	697
viewing.....	696
technical support	
contacting JTAC.....	xxxiv
template	
assigning to a device.....	220, 221
template assignment.....	220, 221
template definition	
cloning.....	186
modifying.....	185
publishing.....	184
unpublishing.....	184
template definition states.....	182
template definitions	
deleting.....	187
inventory viewing.....	185
managing.....	183
specifying device-specific data in.....	200
workflow.....	188
terminal control characters	
for Secure Console.....	108, 109
thresholds	
creating, modifying, and deleting.....	411
topology See network topology	

troubleshoot zip file	
contents	648, 650
download from Junos Space Network Management Platform UI.....	650
download in maintenance mode.....	652
troubleshooting	
device.....	49

U

uninstalling Junos Space application.....	646
unmanaged devices	
adding.....	153
modifying.....	57
unpublishing template definition.....	184
untagging inventory objects.....	697
upgrade	
in-service software	286
upgrading Junos Space application.....	638
upgrading Junos Space Network Management Platform.....	641
upgrading Junos Space software.....	637, 639
Uploading a Device Image	283
user account	
creating in Junos Space.....	509
user administration.....	479
default super administrator.....	480
role assignment, understanding.....	480
roles	
definition.....	480
predefined.....	480, 481
task group.....	481
viewing statistics.....	524
viewing user account information.....	516
See also role-based administration	
user certificate.....	659
user interface	
banner.....	10
global action icons.....	10
User interface	
navigating.....	26
user interface, Junos Space, overview.....	9
user password, changing.....	10
User Preferences icon.....	10
user privileges.....	182
configuration file management.....	445
user-defined role, creating.....	505, 506
user-defined role, deleting.....	507

user-defined role, managing.....	502, 503
creating.....	503
deleting.....	503
overview.....	503

users	
disabling.....	515
enabling.....	515

V

view script details.....	335
viewing charts.....	403
viewing device template definition	
statistics.....	181, 226
viewing device template inventory.....	225
VIP interface	
changing in same subnet.....	561
changing to a different subnet.....	561
multinode	
changing in same subnet.....	561

W

workspace	
Administration.....	551
administrator access.....	479
Audit Logs.....	531
Devices.....	35
DMI Schema Management.....	714
enforcement.....	480
Jobs.....	461
Users.....	480
wwadapter	
installing.....	166
overview.....	165

X

X.509 format certificate.....	663
-------------------------------	-----

