



Junos[®] Space

Network Management Platform User Guide

Release
13.3



Modified: 2016-08-03

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

13.3

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	xxix
	Documentation and Release Notes	xxix
	Documentation Conventions	xxix
	Documentation Feedback	xxxi
	Requesting Technical Support	xxxii
	Self-Help Online Tools and Resources	xxxii
	Opening a Case with JTAC	xxxii
Part 1	Junos Space User Interface	
Chapter 1	Getting Started	3
	Logging In to Junos Space	3
	Changing Your Password on Junos Space	5
	Using the Getting Started Assistants on Junos Space	6
	Accessing Help on Junos Space	7
	Logging Out of Junos Space	7
Part 2	Devices	
Chapter 2	Device Management Overview	11
	Device Management Overview	11
	Device Inventory Overview	12
	Viewing Managed Devices	14
	Understanding How Junos Space Automatically Resynchronizes Managed Devices	17
	Network as System of Record	17
	Junos Space as System of Record	19
	Troubleshooting Devices	19
Chapter 3	Device Configuration	21
	Modifying the Configuration on the Device	21
	Reviewing and Deploying the Device Configuration	25
	Viewing the Configuration Changes on the Device	26
	Validating the Configuration on the Device	27
	View the Device-Configuration Validation Report	28
	Excluding or Including a Group of Configuration Changes	28
	Deleting a Group of Configuration Changes	29
	Approving the Configuration Changes	29

	Rejecting the Configuration Changes	30
	Deploying the Configuration Changes	30
	Viewing the Configuration Change Log	31
	Resolving Out of band Changes	32
	Filtering Devices by CSV	34
	Creating a Quick Template from the Device Configuration	34
	Viewing Assigned Shared Objects	35
	Viewing Template Deployment (Devices)	37
	Viewing Active Configuration	39
	Viewing Device Statistics	40
Chapter 4	Device Inventory	41
	Viewing Physical Inventory	41
	Displaying Service Contract and EOL Data in the Physical Inventory Table	43
	Viewing Physical Interfaces	44
	Viewing Logical Interfaces	45
	Exporting License Inventory	47
	Viewing and Exporting Software Inventory	51
	Exporting Physical Inventory Information	53
	Viewing Associated Scripts	54
	Executing a Promoted Script on a Device	54
	Executing Scripts on a Physical Inventory Component	56
	Executing a Promoted Script on a Physical Inventory	57
	Executing Scripts on a Physical Interface	58
	Executing a Promoted Script on a Physical Interface	59
	Executing Scripts on a Logical Interface	60
	Executing a Promoted Script on a Logical Interface	61
	Applying CLI Configlets to the Physical Inventory	62
	Applying CLI Configlets to Physical Interfaces	63
	Applying CLI Configlets to Logical Interfaces	64
	Viewing Staged Images on a Device	64
	Deleting Staged Images on a Device	65
Chapter 5	Device Operations	67
	Deleting Devices	67
	Resynchronizing Managed Devices with the Network	68
	Using Looking Glass	69
	Understanding Logical Systems for SRX Series Services Gateways	71
	Creating a Logical System (LSYS)	71
	Deleting Logical Systems	72
	Viewing the Physical Device for a Logical System	73
	Viewing Logical Systems for a Physical Device	74
	Putting a Device in RMA State and Reactivating Its Replacement	75
	Putting a Device in RMA State	75
	Reactivating a Replacement Device	76
	Applying CLI Configlets to Devices	76
	Executing Scripts on Devices	77
	Executing Scripts on Devices Locally with JUISE	78
	Modifying the Serial Number of a Device	80
	Rebooting Devices	81

	Creating Device Partitions	82
	Deleting Device Partitions	83
	Modifying Device Partitions	83
Chapter 6	Device Access	85
	Secure Console Overview	85
	Connecting to a Device From Secure Console	86
	Connecting to a Managed Device from the Device Management Page	86
	Connecting to an Unmanaged Device from the Device Management Page	87
	Connecting to a Managed or Unmanaged Device from the Secure Console Page	89
	Launching a Device's Web User Interface	90
	Key-Based Authentication Overview	91
	Generating and Uploading Authentication Keys to Devices	92
	Generating Authentication Keys	92
	Uploading Authentication Keys to Multiple Managed Devices for the First Time	93
	Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space	94
	Resolving Key Conflicts	95
	Changing Device Authentication from Password-based to Key-based Authentication	96
Chapter 7	Device Monitoring	97
	Viewing and Managing Alarms	97
	Viewing Alarms	98
	Using Alarm Filters to View Alarms	99
	Acknowledging Alarms	100
	Clearing Alarms	100
	Escalating Alarms	100
	Unacknowledging Alarms	100
	Viewing Acknowledged Alarms	101
Chapter 8	Custom Attributes	103
	Adding Custom Labels	103
	Adding Custom Labels for a Device	103
	Adding Custom Labels for Physical Inventory	104
	Adding Custom Labels for a Physical Interface	105
	Adding Custom Labels for a Logical Interface	105
	Deleting Custom Labels	106
	Modifying Custom Labels	107
Chapter 9	Discover Devices	109
	Device Discovery Overview	109
	Discovering Devices	111
	Specifying Device Targets	112
	Specifying Probes	113
	Specifying Credentials	114

Chapter 10	Model Devices	117
	Model Devices Overview	117
	Creating Connection Profiles	118
	Creating a Modeled Instance	122
	Modifying Connection Profiles	124
	Deleting Connection Profiles	124
	Viewing the Status of Modeled Devices	125
	Adding More Devices to an Existing Modeled Instance	126
	Viewing and Copying Configlet Data	127
	Downloading a Configlet	127
	Activating Devices by Using Configlets	129
	Activating a Device by Using a Plain-text Single Configlet	129
	Activating a Device by Using an AES-encrypted Single Configlet	130
	Activating a Device by Using a Plain-text Bulk Configlet	130
	Activating a Device by Using an AES-encrypted Bulk Configlet	131
	Deleting Modeled Instances	131
	Cloning a Connection Profile	132
Chapter 11	Unmanaged Devices	133
	Adding Unmanaged Devices	133
	Modifying Unmanaged Device Configuration	136
Chapter 12	Secure Console	137
	Configuring SRX Device Clusters in Junos Space	137
	Configuring a Standalone Device from a Single-node Cluster	137
	Configuring a Standalone Device from a Two-Node Cluster	139
	Configuring a Primary Peer in a Cluster from a Standalone Device	140
	Configuring a Secondary Peer in a Cluster from a Standalone Device	142
Chapter 13	Device Adapter	145
	Worldwide Junos OS Adapter Overview	145
	Installing the Worldwide Junos OS Adapter	146
	Connecting to ww Junos OS Devices	147
Chapter 14	Upload Keys to Devices	149
	Key-Based Authentication Overview	149
	Generating and Uploading Authentication Keys to Devices	149
	Generating Authentication Keys	150
	Uploading Authentication Keys to Multiple Managed Devices for the First Time	151
	Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space	152
Chapter 15	Device Statistics	155
	Viewing Device Statistics	155
Chapter 16	QuickView	157
	Viewing Devices and Logical Systems with QuickView	157

Chapter 17	Configuration Guides	159
	Configuration Guides Overview	159
	Saving the Configuration Created using the Configuration Guides	160
	Deploying the Configuration Created using the Configuration Guides	160
	Previewing the Configuration Created using the Configuration Guides	161
Part 3	Device Templates	
Chapter 18	Overview	165
	Device Templates Overview	165
	Device Templates Overview	165
	Device Templates Workflow	170
	Viewing Template Definition Statistics	171
	User Privileges in Device Templates	172
	Changing Template Definition States	172
Chapter 19	Template Definitions	173
	Creating a Template Definition	173
	Specifying Device-specific Values in Template Definitions	179
	Creating a CSV file with device-specific values	179
	Using a CSV file to set device-specific values	180
	Working with Rules	181
	Finding Configuration Options	183
	Cloning a Template Definition	185
	Deleting a Template Definition	186
	Exporting a Template Definition	186
	Importing a Template Definition	187
	Modifying a Template Definition	188
	Publishing a Template Definition	189
	Managing CSV Files for a Template Definition	190
	Unpublishing a Template Definition	191
Chapter 20	Device Templates	193
	Creating a Device Template	193
	Deploying a Template	195
	Undeploying a Device Template	197
	Deleting a Device Template	198
	Modifying a Device Template	199
	Assigning a Device Template to Devices	199
	Unassigning a Device Template From Devices	200
	Viewing Template Deployment Details (Device Templates)	201
	Auditing a Device Template Configuration	202
	Viewing Device Template Statistics	203
Chapter 21	Quick Templates	205
	Quick Templates Overview	205
	Creating a Quick Template	206
	Deploying a Quick Template	210

Part 4	CLI Configlets	
Chapter 22	CLI Configlets Overview	215
	CLI Configlets Overview	215
	Configlet Variables	216
	Default Variables	216
	User defined Variables	216
	Predefined Variables	216
	Velocity Templates	216
	CLI Configlets Workflow	216
	Configlets User Roles	219
	Configlet Context	220
	Context of an Element	221
	Context filtering	221
	Nesting Parameters	223
Chapter 23	Managing CLI Configlets	225
	Creating a CLI Configlet	225
	Applying a CLI Configlet to a Device	228
	Cloning a CLI Configlet	229
	Deleting CLI configlets	230
	Importing a CLI Configlet	230
	Modifying CLI Configlets	231
	Exporting CLI Configlets	232
	Comparing CLI Configlet Versions	232
	Viewing CLI Configlet Statistics	234
	CLI Configlet Examples	234
	CLI Configlet Examples	234
	Example 1 - Setting the description of a physical interface	235
	Example 2 - Setting the vlan of a logical interface, where the vlan id is chosen from a predefined set of values	235
	Example 3 - Setting a description on all the interfaces of a device	237
	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	238
	Example 5 - Halting the description of a physical interface	240
Chapter 24	Configuration Views Overview	243
	Configuration Views Overview	243
	Configuration View Variables	244
	Configuration View Workflow	244
	Configuration Views User Roles	246
	XML Extensions	246
Chapter 25	Managing Configuration Views	249
	Creating a Configuration View	249
	Modifying a Configuration View	251
	Deleting Configuration Views	251

	Viewing Configuration Views Statistics	252
	Default Configuration Views Examples	252
	Default view	253
	Example XML view	253
	Example Form view	254
	Example Form view	254
Chapter 26	XPath and Regex	257
	XPATH and Regex Overview	257
	Creating Xpath or Regex	257
	Modifying Xpath and Regex	258
	Deleting Xpath and Regex	258
	XPath and Regular Expression Examples	259
	Example 1 – Alphanumeric	259
	Example 2 – Logical Interfaces per Physical Interface	259
	Example 3 – Physical Interfaces	259
	Example 4 – Devices	260
Chapter 27	Configuration Filter	261
	Creating a Configuration Filter	261
	Modifying a Configuration Filter	262
	Deleting Configuration Filters	262
Part 5	Images and Scripts	
Chapter 28	Overview	265
	Device Images and Scripts Overview	265
	User Roles	266
Chapter 29	Device Images	273
	Device Images Overview	273
Chapter 30	Scripts	275
	Scripts Overview	275
	Promoting Scripts Overview	279
Chapter 31	Operations	281
	Operations Overview	281
Chapter 32	Script Bundles	283
	Script Bundles Overview	283
Chapter 33	Configuration: Device Images	285
	Uploading Device Images to Junos Space	285
	Staging Device Images	286
	Viewing Device Association of Images	289
	Verifying the Checksum	290
	Deploying Device Images	293
	Viewing Device Image Deployment Results	302
	Deleting Device Images	303

	Modifying Device Image Details	307
	Viewing and Deleting MD5 Validation Results	308
	Viewing the MD5 Validation Results	308
	Deleting the MD5 Validation Results	309
Chapter 34	Configuration: Scripts	311
	Modifying a Script	311
	Modifying Script Types	314
	Comparing Script Versions	314
	Deleting Scripts	315
	Staging Scripts on Devices	316
	Viewing Device Association of Scripts	319
	Verifying the Checksum of Scripts on Devices	320
	Enabling Scripts on Devices	321
	Disabling Scripts on Devices	324
	Disabling Scripts on Devices	326
	Removing Scripts from Devices	328
	Executing Scripts on Devices	331
	Viewing Execution Results	333
	Importing Scripts	334
Chapter 35	Configuration: Operations	337
	Creating an Operation	337
	Modifying an Operation	340
	Running an Operation	341
	Copying an Operation	342
	Deleting an Operation	343
	Exporting an Operation in .tar Format	344
	Importing an Operation	345
Chapter 36	Configuration: Script Bundles	347
	Creating a Script Bundle	347
	Modifying a Script Bundle	349
	Deleting Script Bundles	350
	Staging Script Bundles on Devices	350
	Executing Script Bundles on Devices	353
	Enabling Scripts in Script Bundles on Devices	355
	Disabling Scripts in Script Bundles on Devices	356
Chapter 37	Administration: Scripts	359
	Viewing Script Details	359
	Viewing Verification Results	360
	Exporting Scripts in .tar Format	361
	Scripts User Roles	362
Chapter 38	Administration: Operations	363
	Viewing Operations Results	363
Chapter 39	Administration: Script Bundles	365
	Viewing Device Associations of Scripts in Script Bundles	365

Chapter 40	Annotations and Examples	367
	Scripts Annotations	367
	Script Execution Types	369
	Variable Context	369
	Local Script Execution	370
	Nesting variables	370
	Script Example	371
Part 6	Reports and Report Definitions	
Chapter 41	Report Definitions	375
	Reports Overview	375
	Creating Report Definitions	382
	Managing Report Definitions	383
	Modify Report Definitions	384
	Cloning Report Definitions	384
	Deleting Report Definitions	384
	Viewing Report Definitions	384
Chapter 42	Reports	387
	Generating Reports	387
	Viewing Generated Reports	388
	Deleting Generated Reports	389
Part 7	Network Monitoring	
Chapter 43	Network Monitoring Overview	393
	Network Monitoring Workspace Overview	394
	Network Monitoring Reports Overview	397
	Resource Graphs	397
	Key SNMP Customized Performance Reports, Node Reports, and Domain Reports	397
	Database Reports	397
	Statistics Reports	397
Chapter 44	Monitoring Devices and Assets	399
	Viewing the Node List	399
	Resyncing Nodes	400
	Turning SNMP Data Collection Off and On	401
	Searching in the Network Monitoring Workspace	402
	Viewing the Dashboard	403
	Tracking and Searching for Assets	405
	Working with Topology	406
	Using the Search Option to View Nodes	407
	Working with Topology Map Views	407
	Viewing Alarms and Node Details for Nodes	408
	Viewing Nodes with Active Alarms	409
	Managing Alarms Associated with Nodes	410
	Viewing the Topology Map with Different Layouts	410
	Automatic Refresh of Topology Map	410

	Pinging a Node	411
	Viewing the Alarms Associated with the Node	411
	Viewing the Events Associated with the Node	411
	Viewing the Resource Graphs Associated with the Node	412
Chapter 45	Working With Events, Alarms, and Notifications	413
	Viewing and Tracking Outages	413
	Viewing and Managing Events	414
	Events Landing Page	414
	Advanced Event Search	415
	Viewing the Events List	415
	Viewing Event Details	416
	Using Event Filters to View Events	417
	Viewing and Managing Alarms	417
	Viewing Alarms	418
	Using Alarm Filters to View Alarms	420
	Acknowledging Alarms	420
	Clearing Alarms	420
	Escalating Alarms	421
	Unacknowledging Alarms	421
	Viewing Acknowledged Alarms	421
	Viewing, Configuring, and Searching for Notifications	421
	Notification Escalation	422
Chapter 46	Working With Reports and Charts	423
	Creating Reports	423
	Creating Key SNMP Customized Performance Reports, Node Reports, and Domain Reports	423
	Creating a New KSC Report from an Existing Report	424
	Viewing Reports	424
	Viewing Resource Graphs	425
	Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports	425
	Viewing Database Reports	426
	Sending Database Reports	426
	Viewing Pre-run Database Reports	427
	Viewing Statistics Reports	427
	Generating a Statistics Report for Export	428
	Deleting Reports	429
	Deleting Key SNMP Customized Reports	429
	Deleting Pre-Run Database Reports	429
	Viewing Charts	429
Chapter 47	Managing Network Monitoring System	431
	Admin: Configuring Network Monitoring	431
	Network Monitoring System: System Information	431
	Generating a Log File for Troubleshooting	432

	Notification Status	432
	Updating Network Monitoring After Upgrading the Junos Space Network Management Platform	433
	Overview	433
	Step 1: Monitoring the Software Install Status Window for File Conflicts	433
	Step 2: Identifying Files with Conflicts	434
	Step 3: Merging Files with Conflicts	436
	Step 4: Verifying the Manual Merge Status of Configuration Files	437
	Step 5: Final Steps After Upgrading Network Monitoring	437
Chapter 48	Managing Network Monitoring Operations	439
	Configuring SNMP Community Names by IP	439
	Configuring SNMP Data Collection per Interface	440
	Managing and Unmanaging Interfaces and Services	441
	Managing Thresholds	441
	Creating Thresholds	441
	Modifying Thresholds	444
	Deleting Thresholds	445
	Selecting and Sending an Event to the Network Management System	445
	Configuring Notifications	446
	Configuring Event Notifications	446
	Configure Destination Paths	448
	Configure Path Outages	449
	Configuring Scheduled Outages	449
	Compiling SNMP MIBs	450
	Uploading MIBs	450
	Compiling MIBs	451
	Viewing MIBs	451
	Deleting MIBs	451
	Clearing MIB Console Logs	452
	Generating Event Configuration	452
	Generating a Data Collection Configuration	453
	Managing Events Configuration Files	455
	Adding New Events Configuration Files	455
	Deleting Events Configuration Files	456
	Modifying Events Configuration Files	456
	Managing SNMP Collections	457
	Adding a New SNMP Collection	457
	Modifying an SNMP Collection	458
	Managing Data Collection Groups	458
	Adding New Data Collection Files	458
	Deleting Data Collection Files	459
	Modifying Data Collection Files	459
Chapter 49	Managing Devices	463
	Managing Surveillance Categories	463
	Modifying Surveillance Categories	463
	Deleting Surveillance Categories	463
	Adding Surveillance Categories	464

Chapter 50	Configuring Alarm Notifications	465
	Alarm Notification Configuration Overview	465
	Basic Filtering	465
	Guidelines for Configuring Alarm Notifications	466
	Advanced Filtering	466
	Configuring Alarm Notification	468
	Configuring a Basic Filter for Alarm Notification	468
	Activating Alarm Notification Configuration Files for Basic Filtering	469
	Reloading a Filter Configuration to Apply Filter Configuration Changes	470
Part 8	Configuration Files	
Chapter 51	Manage Configuration Files	473
	Managing Configuration Files Overview	473
	User Privileges in Configuration File Management Overview	475
	Viewing Configuration File Statistics and Inventory	476
	Deleting Configuration Files	477
	Restoring Configuration Files	478
	Comparing Configuration Files	480
	Editing Configuration Files	482
	Exporting Configuration Files	484
Chapter 52	Backup Config Files	487
	Backing Up Configuration Files	488
Part 9	Jobs	
Chapter 53	Overview	495
	Jobs Overview	495
Chapter 54	Manage Jobs	499
	Viewing Your Jobs	499
	Viewing Scheduled Jobs	500
	View	500
	Viewing Job Types	500
	Viewing Job Status Indicators	500
	Viewing Job Details, Status, and Results	501
	Executing Commands on Jobs	502
	Viewing Statistics for Scheduled Jobs	503
	Viewing the Types of Jobs That Are Run	503
	Viewing the State of Jobs That Have Run	503
	Viewing Average Execution Times for Jobs	504
	Viewing Objects on Which a Job is Executed	504
	Reassigning Jobs	506
	Canceling a Job	509
	Deleting Your Jobs	510
	Viewing Database Backup Job Recurrence	510
	Retrying a Job on Failed Devices	511

Chapter 55	Archive Jobs	513
	Archiving and Purging Jobs	513
	Archiving Jobs to a Local Server and Purging the Jobs from the Database	513
	Archiving Jobs to a Remote Server and Purging the Jobs from the Database	514
Part 10	Users	
Chapter 56	Manage Roles	519
	Role-Based Access Control Overview	519
	Authentication	519
	RBAC Enforcement	520
	Enforcement by Workspace	520
	RBAC Enforcement Not Supported for Getting Started Page	520
	Configuring Users to Manage Objects in Junos Space Overview	521
	Predefined Roles Overview	521
	Managing Roles Overview	550
	Managing Roles	551
	Viewing User Role Details	551
	Performing Manage Roles Commands	551
Chapter 57	Manage User-Defined Roles	553
	Creating a User-Defined Role	553
	Modifying User-Defined Roles	554
	Deleting User-Defined Roles	555
Chapter 58	Manage Domains	557
	Managing Domains Overview	557
	Working with Domains	564
	Adding a Domain	564
	Modifying a Domain	566
	Deleting Domains	567
Chapter 59	Manage Users	571
	Creating User Accounts	571
	Creating a New User Account	572
	Limiting User Sessions	579
	Disabling and Enabling Users	581
	Viewing Users	582
	Sorting Columns	583
	Displaying or Hiding Columns	583
	Filtering on Columns	584
	Viewing User Details	585
	Performing Actions on Users	586
	Modifying a User	587
	Deleting Users	590
	Unlocking Users	592
	Changing Your Password on Junos Space	593
	Clearing User Local Passwords	594

	Viewing User Statistics	595
	Viewing the Number of Users Assigned by Role	595
Chapter 60	Manage Remote Profiles	597
	Creating a Remote Profile	597
Chapter 61	User Sessions	599
	Terminating User Sessions	599
Part 11	Audit Logs	
Chapter 62	View	603
	Junos Space Audit Logs Overview	603
	Viewing Audit Logs	604
	Viewing Audit Log Statistics	606
	Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel	608
Chapter 63	Archive / Purge	611
	Archiving and Purging Audit Logs	611
	Archiving Audit Logs to a Local Server and Purging the Logs from the Database	611
	Archiving Audit Logs to a Remote Server and Purging the Logs from the Database	612
Chapter 64	Export	615
	Exporting Audit Logs	615
Part 12	Administration	
Chapter 65	Overview	619
	Junos Space Administrators Overview	619
	Maintenance Mode Overview	621
	Maintenance Mode Access and System Locking	621
	Maintenance-Mode User Administration	622
	Running Applications in Separate Server Instances	622
	Adding a Server Group	623
	Adding a Server to a Server Group	624
	Starting Servers in a Server Group	625
	Stopping Servers in a Server Group	625
	Removing a Server Group	625
	Moving an Application to a Different Server Group	626
Chapter 66	Fabric	627
	Fabric Management	627
	Fabric Management Overview	627
	Single-Node Functionality	628
	Multinode Functionality	629
	Specialized Node Functionality	632

Node Function Availability	634
Adding a Node to an Existing Junos Space Fabric	635
Viewing Nodes in the Fabric	637
Changing Views	637
Viewing Fabric Node Details	638
Performing Fabric Node Actions	640
Configuring the Network Settings of a Node in the Junos Space Fabric	641
Network Settings Configuration Guidelines	642
Changing the VIP Interface in the Same Subnet	642
Changing the Node Management IP in the Same Subnet	642
Changing the Default Gateway	642
Changing the Management IP to a Different Network	643
Adding the Device Management IP Address	643
Changing the Device Management IP Address in the Same Subnet . .	644
Changing the Device Management IP Address to a Different Network	644
Deleting a Device Management IP Address	644
Changing the VIP Interface to a Different Network	645
Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet	645
Changing the VIP Interface of a Multiple-Node Fabric to a Different Network	645
Shutting Down or Rebooting a Junos Space Appliance Node From Junos Space	646
Deleting a Node from the Junos Space Fabric	647
Replacing a Failed Junos Space Node	649
Overall System Condition and Fabric Load History Overview	649
Overall System Condition	649
Fabric Load History	651
Active Users History	651
Monitoring Nodes in the Fabric	652
Viewing and Modifying the SNMP Configuration for a Fabric Node . .	654
Starting SNMP Monitoring on Fabric Nodes	675
Stopping SNMP Monitoring on Fabric Nodes	676
Restarting SNMP Monitoring on Fabric Nodes	676
Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node . . .	677
Adding a Third-Party SNMP V3 Manager on a Fabric Node	677
Deleting a Third-Party SNMP Manager from a Fabric Node	678
Creating a System Snapshot	679
Deleting a System Snapshot	681
Restoring the System to a Snapshot	681

Chapter 67	Managing Databases	683
	Backing Up and Restoring the Database Overview	684
	Backing Up a Database	685
	Restoring a Database	685
	Backing Up the Junos Space Network Management Platform Database	686
	Backing Up the Junos Space Network Management Platform Database to a Local Directory	687
	Backing Up the Junos Space Network Management Platform Database to a Remote Host	690
	Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface	692
	Restoring a Local Junos Space Network Management Platform Database Through the Junos Space User Interface	693
	Restoring the Junos Space Network Management Platform Database from a Remote File Through the Junos Space User Interface	694
	Viewing Database Backup Files	696
	Changing Views	696
	Viewing Database Details	696
	Managing Database Commands	697
	Deleting Junos Space Network Management Platform Database Backup Files	698
	Viewing Database Backup Job Recurrence	699
Chapter 68	Manage Licenses	701
	Generating and Uploading the Junos Space License Key File	701
	Generating the Junos Space License Key File	702
	Uploading the Junos Space License Key File Contents	702
	Viewing Licenses	703
	Viewing License Details	703
Chapter 69	Manage Applications	705
	Managing Applications Overview	705
	Managing Junos Space Applications	706
	Installing or Upgrading a Junos Space Application	707
	Viewing Detailed Information About the Junos Space Application	707
	Performing Actions on the Junos Space Applications	708
	Modifying Junos Space Application Settings	709
	Modifying Network Management Platform Settings	711
	Configuring Password Rules for Junos Space Network Management Platform	714
	Managing Services	718
	Configuring Network Activate Application Settings	721
	Adding a Junos Space Application	721
	Junos Space Software Upgrade Overview	724
	Upgrading a Junos Space Application	725
	Upgrading Junos Space Software Overview	727
	Junos Space 13.3R1 Release Highlights	727
	Before You Begin	728
	Upgrading Junos Space Release to Release 13.3R1 and Later Versions	728

	Upgrading Junos Space Network Management Platform	729
	Uninstalling a Junos Space Application	733
Chapter 70	Troubleshoot Space	735
	System Status Log File Overview	735
	System Status Log File	735
	Customizing Status Log File Content	736
	Downloading System Log Files for a Junos Space Appliance	736
	Customizing Log Files to Download	736
	Customizing Node System Status Log Checking	737
	Customizing Node Log Files To Download	738
	Downloading the Troubleshooting Log File in the Server Mode	738
	Downloading the Troubleshooting Log File in the Maintenance Mode	740
	Downloading Troubleshooting System Log Files Through the CLI	740
	Downloading a System Log File by Using a USB Device	741
	Downloading System Log File by Using SCP	742
Chapter 71	Manage Certificates	745
	Certificate Management Overview	745
	Workflow	745
	Loading a Custom Junos Space Server Certificate	747
	Loading a User Certificate	747
	Loading CA Certificates and CRLs	748
	Changing the Authentication Mode	749
	Invalid Certificates	750
	Installing Custom SSL Certificate on the Junos Space Server	751
	Changing the Default Junos Space Server SSL Certificate	751
	Installing an X.509 Junos Space Server Certificate	751
	Installing a PKCS #12 Format Junos Space Server Certificate	752
	Certificate Expiry	753
	Certificate Attributes	753
Chapter 72	Manage Authentication Servers	757
	Remote Authentication Overview	757
	Junos Space Authentication Modes Overview	758
	Local Authentication	758
	Remote Authentication	758
	Remote-Local Authentication	759
	Managing Remote Authentication Servers	759
	Creating a Remote Authentication Server	760
	Modifying Authentication Settings	763
	Configuring a RADIUS Server for Authentication and Authorization	764
	Configuring TACACS+ for Authentication and Authorization	768
	Junos Space Login Behavior with Remote Authentication Enabled	770
Chapter 73	Manage SMTP Servers	775
	Managing SMTP Servers	775
	Adding an SMTP Server	776

Chapter 74	Manage Tags	779
	Tags Overview	779
	Tags Overview	780
	Managing Tags	781
	Managing Tags	781
	Managing Hierarchical Tags	783
	Using the Tag Hierarchy Pane	784
	Using the Tabular View Pane	788
	Sharing a Tag	789
	Renaming Tags	790
	Deleting Tags	791
	Tagging an Object	793
	Viewing Tags for a Managed Object	794
	Untagging Objects	794
	Filtering the Inventory by Using Tags	795
	Viewing Tagged Objects	796
	Creating Tags	798
	Creating a Tag	798
Chapter 75	Manage DMI Schemas	803
	Managing DMI Schemas Overview	804
	Updating a DMI Schema	806
	Creating a Compressed Tar File for Updating DMI Schema	809
	Setting a Default DMI Schema	813
	Troubleshooting DMI Schema Management	814
Chapter 76	Generate Key	817
	Key-Based Authentication Overview	817
	Generating and Uploading Authentication Keys to Devices	817
	Generating Authentication Keys	818
	Uploading Authentication Keys to Multiple Managed Devices for the First Time	819
	Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space	820
Part 13	Systems of Record and Disaster Recovery	
Chapter 77	Systems of Record and Disaster Recovery	825
	Systems of Record in Junos Space Overview	825
	Systems of Record	825
	Implications	826
	Disaster Recovery Overview	826
	Overview	827
	Prerequisites	827
	Creating the DR Master Cluster	828
	1. Configuring the DR Master Cluster	829
	2. Starting the Backup for the DR Master Cluster	830
	3. Stopping the Backup	831

	Creating the DR Slave Cluster	831
	1. Configuring the DR Slave Cluster	832
	2. Starting to Pull the Backups From the DR Master	833
	3. Stopping Pulling the Backups from the DR Master	834
	4. Restoring	835
	Performing a Reverse Restore	836
Part 14	Index	
	Index	839

List of Figures

Part 2	Devices	
Chapter 2	Device Management Overview	11
	Figure 1: Device Management Page	14
	Figure 2: Resynchronization Process	18
Chapter 12	Secure Console	137
	Figure 3: Validating the Server Key Fingerprint	138
Part 3	Device Templates	
Chapter 18	Overview	165
	Figure 4: Workflow for Device Template Definition and Template Creation	171
Part 11	Audit Logs	
Chapter 62	View	603
	Figure 5: Formatting the Local Times Column in Microsoft Excel	609
Part 12	Administration	
Chapter 66	Fabric	627
	Figure 6: Fabric Nodes	628
	Figure 7: Fabric with One Node	630
	Figure 8: Fabric with Two Nodes	631
	Figure 9: Fabric with Three Nodes	632
	Figure 10: Overall System Condition Gauge	650
	Figure 11: Fabric Load History Chart	651
	Figure 12: Active Users History Chart	652
	Figure 13: Disk Usage Threshold Is Normal	656
	Figure 14: Trap Details When Disk Usage Normal	656
	Figure 15: Disk Usage Threshold Exceeds Configured Threshold	656
	Figure 16: Trap Details When Disk Usage Exceeds Configured Threshold	656
	Figure 17: CPU Load Average Threshold Is Normal	659
	Figure 18: Trap Details When CPU Load Average Threshold Is Normal	659
	Figure 19: CPU Load Average Threshold – Upper Limit Exceeded	659
	Figure 20: Trap Details When CPU Load 5 Minute Average Exceeds Threshold	659
	Figure 21: NMA Is Up	661
	Figure 22: Trap Details When NMA Is Up	661
	Figure 23: NMA is Down	661
	Figure 24: Trap Details When NMA is Down	661

Figure 25: WebProxy Is Up	662
Figure 26: Trap Details When WebProxy Is Up	662
Figure 27: WebProxy Is Down	662
Figure 28: Trap Details When WebProxy Is Down	662
Figure 29: JBoss Is Up	663
Figure 30: Trap Details When JBoss Is Up	663
Figure 31: JBoss Is Down	663
Figure 32: Trap Details When JBoss Is Down	663
Figure 33: Mysql Is Up	664
Figure 34: Trap Details When Mysql Is Up	664
Figure 35: Mysql Is Down	664
Figure 36: Trap Details When Mysql Is Down	664
Figure 37: Postgresql Is Up	665
Figure 38: Trap Details When Postgresql Is Up	665
Figure 39: Postgresql Is Down	665
Figure 40: Trap Details When Postgresql Is Down	665
Figure 41: Swap Memory Usage Is Normal	666
Figure 42: Trap Details When Swap Memory Is Normal	666
Figure 43: Swap Memory Usage Threshold Exceeds Upper Limit	666
Figure 44: Trap Details When Swap Memory Usage Exceeds Upper Limit	666
Figure 45: CPU Fan Speed Normal	669
Figure 46: Trap Details When CPU Fan Speed Is Normal	669
Figure 47: CPU Fan Speed Is Below the Configured Threshold	669
Figure 48: Trap Details When CPU Fan Speed Is Below the Configured Threshold	669
Figure 49: CPU Voltage Normal	671
Figure 50: Trap Details When CPU Voltage Is Normal	671
Figure 51: CPU Voltage Is Lower Than Configured Threshold	671
Figure 52: Trap Details When CPU Voltage Is Lower Than Configured Threshold	671
Figure 53: CPU Temperature Normal	672
Figure 54: Trap Details When CPU Temperature Is Normal	672
Figure 55: CPU Temperature Exceeds The Configured Threshold	672
Figure 56: Trap Details When CPU Temperature Exceeds The Configured Threshold	672
Figure 57: Trap Details Junos Space Node Is Down	674
Figure 58: Trap Details Junos Space Node Is Up	674
Figure 59: Trap Details Junos Space Node Is Deleted	674
Figure 60: Network Monitoring Details for the Selected Fabric Node	676

List of Tables

	About the Documentation	xxix
	Table 1: Notice Icons	xxx
	Table 2: Text and Syntax Conventions	xxx
Part 2	Devices	
Chapter 2	Device Management Overview	11
	Table 3: Fields in the Device Management Table	15
Chapter 3	Device Configuration	21
	Table 4: Selected Devices Columns	26
	Table 5: Tabs to View Configuration Deltas	27
	Table 6: Configuration Change Log	32
	Table 7: Resolving Out-of-Band Changes	32
	Table 8: View Assigned Shared Objects Table	36
Chapter 4	Device Inventory	41
	Table 9: Physical Interfaces Columns	44
	Table 10: Logical Interfaces Columns	46
	Table 11: License Usage Summary Fields	49
	Table 12: License Feature or SKU Fields	50
	Table 13: Additional Fields in CSV Files	50
	Table 14: Software Inventory Fields	52
	Table 15: View Staged Images Page	65
Chapter 7	Device Monitoring	97
	Table 16: Information Displayed in the Alarms List	99
Chapter 11	Unmanaged Devices	133
	Table 17: SNMP V3 Configuration Parameters	134
	Table 18: Sample CSV for Importing Unmanaged Devices	134
Part 3	Device Templates	
Chapter 18	Overview	165
	Table 19: Templates Page	165
	Table 20: Device Template States	166
	Table 21: Definitions Page	166
	Table 22: Data Types and Tabs	169
	Table 23: Data Types and Validation Parameters	170
Chapter 20	Device Templates	193
	Table 24: Review Changes Page	197

	Table 25: View Deployment Table	201
Part 4	CLI Configlets	
Chapter 22	CLI Configlets Overview	215
	Table 26: Parameters for a Configlet	217
	Table 27: Attributes of Configlet Parameters	218
	Table 28: Configlets User Roles Permissions	219
	Table 29: Commands to View XML from the CLI	220
Chapter 25	Managing Configuration Views	249
	Table 30: Configuration Views Page Columns	249
	Table 31: Parameters	254
	Table 32: Parameters	255
	Table 33: Parameters and Configured Value Xpath	255
Part 5	Images and Scripts	
Chapter 28	Overview	265
	Table 34: Images and Scripts User Roles	266
Chapter 29	Device Images	273
	Table 35: Images Page	273
Chapter 30	Scripts	275
	Table 36: Scripts Page Fields Description	276
Chapter 33	Configuration: Device Images	285
	Table 37: Routing Platforms and Software Releases Supporting ISSU	294
	Table 38: Select Devices Table Field Descriptions	296
	Table 39: Common Deployment Options Descriptions	298
	Table 40: Conventional Deployment Options Descriptions	298
	Table 41: Unified ISSU Deployment Options Descriptions	299
	Table 42: Advanced Deployment Options Descriptions	300
	Table 43: Remove Image from Staged Devices Page Information	305
	Table 44: Validation Results Page Field Descriptions	309
Chapter 34	Configuration: Scripts	311
	Table 45: View Execution Results Page Fields Description	334
Chapter 35	Configuration: Operations	337
	Table 46: Create Operation Dialog Box Icon Descriptions	339
Chapter 36	Configuration: Script Bundles	347
	Table 47: Create Script Bundle Dialog Box Icon Descriptions	348
	Table 48: Modify Script Bundle Dialog Box Icon Descriptions	349
Chapter 37	Administration: Scripts	359
	Table 49: Script Details Dialog Box Fields	359
	Table 50: Script Verification Results Page Fields	361
	Table 51: Scripts User Roles	362

Part 6	Reports and Report Definitions	
Chapter 41	Report Definitions	375
	Table 52: Audit Trail Report Definition Attributes	376
	Table 53: Device Inventory Report Definition Attributes	376
	Table 54: Device License Inventory Report Definition Attributes	377
	Table 55: Device Logical Interface Inventory Report Definition Attributes	378
	Table 56: Device Physical Interface Inventory Report Definition Attributes	379
	Table 57: Device Physical Inventory Report Definition Attributes	379
	Table 58: Device Software Inventory Report Definition Attributes	380
	Table 59: Job Inventory Report Definition Attributes	381
Part 7	Network Monitoring	
Chapter 44	Monitoring Devices and Assets	399
	Table 60: Alarms Table	404
	Table 61: Notifications Table	404
	Table 62: Node Status Table	405
	Table 63: Resource Graphs Table	405
	Table 64: Topology Map Options	407
Chapter 45	Working With Events, Alarms, and Notifications	413
	Table 65: Information Displayed in the Alarms List	419
Part 9	Jobs	
Chapter 53	Overview	495
	Table 66: Junos Space Job Types Per Application	496
Chapter 54	Manage Jobs	499
	Table 67: Job Icon Status Indicators	500
	Table 68: Job Details and Columns in the Jobs Table	501
	Table 69: Jobs that Support Viewing Objects on Which a Job is Executed	505
Part 10	Users	
Chapter 56	Manage Roles	519
	Table 70: Predefined Roles for the Junos Space Network Management Platform	522
	Table 71: Predefined Roles for the Network Activate Application	539
	Table 72: Predefined Roles for the Service Insight Application	541
	Table 73: Predefined Roles for the Service Now Application	543
	Table 74: Predefined Roles for the Ethernet Design Application	549
Chapter 58	Manage Domains	557
	Table 75: Actions Supported on Device Partitions	560
Chapter 59	Manage Users	571
	Table 76: Differences Between Temporary and Regular Passwords	572
	Table 77: User Detail Summary Page	585

Part 11	Audit Logs	
Chapter 62	View	603
	Table 78: Detailed Audit Logs Information and Audit Log Table Columns	604
	Table 79: Audit Log Details for Recurring and Nonrecurring Jobs	605
Part 12	Administration	
Chapter 65	Overview	619
	Table 80: Junos Space Administrators and Junos Space User Interface Users	619
Chapter 66	Fabric	627
	Table 81: Fields for the Fabric Monitoring Inventory Page	638
	Table 82: Logical Component Monitoring	652
	Table 83: SNMP Configuration Parameters: Monitoring Disk Usage	655
	Table 84: SNMP Configuration Parameters: Monitoring the CPU Load Average	658
	Table 85: SNMP Configuration Parameters: Monitoring Processes	661
	Table 86: SNMP Configuration Parameters: Monitoring Linux Hardware	667
Chapter 67	Managing Databases	683
	Table 87: Backup Schedule Units and Increments	689
	Table 88: Fields in the Manage Databases Table	697
Chapter 68	Manage Licenses	701
	Table 89: Licenses Details	703
Chapter 69	Manage Applications	705
	Table 90: Application Information	707
	Table 91: Junos Space Network Management Platform Application Settings	711
	Table 92: Password Constraint Parameters	715
	Table 93: Starting, Stopping, and Restarting Network Monitoring	718
	Table 94: Network Activate Application Settings	721
Chapter 70	Troubleshoot Space	735
	Table 95: Log Files included in the troubleshoot File	736
	Table 96: Data and Log Files in troubleshooting log File	739
Chapter 71	Manage Certificates	745
	Table 97: Certificate Attributes	754
Chapter 72	Manage Authentication Servers	757
	Table 98: Remote Authentication Server Settings	761
	Table 99: TACACS+ Remote Authentication Server Settings	768
Chapter 74	Manage Tags	779
	Table 100: Tag Information	782
	Table 101: Objects Supported on the View Tagged Objects Page	797
Chapter 75	Manage DMI Schemas	803
	Table 102: Sample URLs for the Repository	810
	Table 103: Schema Name Mapping Information	812

About the Documentation

- Documentation and Release Notes on page xxix
- Documentation Conventions on page xxix
- Documentation Feedback on page xxxi
- Requesting Technical Support on page xxxii

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 xxx 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 xxx 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](#)

CHAPTER 1

Getting Started

- [Logging In to Junos Space on page 3](#)
- [Changing Your Password on Junos Space on page 5](#)
- [Using the Getting Started Assistants on Junos Space on page 6](#)
- [Accessing Help on Junos Space on page 7](#)
- [Logging Out of Junos Space on page 7](#)

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.

Juniper Networks recommends a screen resolution that is 1280 x 1024 pixels or higher.



WARNING: To avoid a Browser Exploit Against SSL/TLS (BEAST) attack, whenever you log in to Junos Space through 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 log in to Junos Space, ensure that the Adobe Flash version 10 or later plug-in is installed in your browser.



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 bar of your browser window, enter **https://virtual-IP-address/mainui/**, where *virtual-IP-address* is previously configured virtual IP (VIP) address that is used for Web access to Junos Space.

2. Press Enter or click **Search**.

The Junos Space login page appears.

3. In the **Username** text box, enter your username. The default username is **super**. For information about how to change your username, consult your system administrator.
4. In the **Password** text box, enter your password. The default password is **juniper123**. For information about how to change your password, see [“Changing Your Password on Junos Space” on page 5](#).
5. (Optional) Perform remote authentication by using a challenge/response algorithm configured on the server.

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

6. Click **Log In**.

The Junos Space Network Management Platform Dashboard appears.



NOTE: By default, Junos Space Network Management Platform authenticates a user's username and password. However, you can also use certificates to authenticate and authorize sessions among various servers and users. To configure certificate-based authentication, see [“Certificate Management Overview” on page 745](#) in the *Junos Space Network Management Platform User Guide*.

For more information about the Junos Space Network Management Platform user interface, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

Related Documentation

- [Logging Out of Junos Space on page 7](#)

Changing Your Password on Junos Space

After you log in to Junos Space Network Management Platform, you can change your password through the User Preferences icon on the Junos Space banner. You do not require any particular Junos Space role to change your password.

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



NOTE: When you upgrade to Junos Space Network Management Platform 12.1 or later, the default standard takes effect immediately. All local users receive password expiration messages the first time they log in to Junos Space after the update.



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



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

To change your local password:

1. On the Junos Space Network Management Platform user interface, click the User Preferences icon on the right side of the Junos Space application banner.

The Change Local Password and Certificate dialog box appears.

2. In the **Old Password** text box, enter your old password.



NOTE: Display the rules for password creation by mousing over the information icon (small blue *i*) next to the **New Password** text box.

3. In the **New Password** text box, enter your new password.
4. In the **Confirm Password** text box, enter your new password again to confirm it.



NOTE: The fields on the X.509 Certificate tab are applicable when you want to use certificate-based authentication. If you are using password-based authentication, you can ignore these fields. For more information about certificate-based authentication, see [“Certificate Management Overview” on page 745](#) in the *Junos Space Network Management Platform User Guide*.

5. Click **OK**.

You are logged out of the system. To log in to Junos Space again, you need to use your new password. Other sessions logged in with the same username are unaffected until the next login.

Related Documentation • [Logging In to Junos Space on page 3](#)

Using the Getting Started Assistants on Junos Space

The Getting Started assistants display steps and help on how to complete common tasks, such as increasing the storage capacity. Getting Started appears in the sidebar when you log in to Junos Space only if the **Show Getting Started on Startup** check box at the bottom of the sidebar is selected. If the sidebar is not shown, you can display it by selecting the Help icon in the Junos Space banner.


The Getting Started topics are context-sensitive per application. Getting Started displays all the steps of 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 from the **Applications** list above the task tree.
2. In the sidebar, expand **Getting Started**.

A main Getting Started topic link appears on the sidebar.

If the sidebar is not displayed, select the Help () icon at the right side of the Junos Space header. The sidebar appears.

3. Select a main topic.

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

4. Perform a specific step by clicking the link.

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

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

Related Documentation • [Accessing Help on Junos Space on page 7](#)

Accessing Help on Junos Space

Junos Space provides 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. Help topics appear as links on the sidebar.

To access online Help:

1. Click the workspace within which you want to work.
2. Click the Help icon at the right side of the Junos Space header.

The help icon is represented as .

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  icon at the top right of the side bar to hide it.

For more information about the Junos Space Network Management Platform user interface, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

Related Documentation • [Using the Getting Started Assistants on Junos Space on page 6](#)

Logging Out of Junos Space

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

To log out of Junos Space, click the **Log Out** icon on 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** (from the Actions menu) > **User > Automatic logout after inactivity (minutes)** to modify the logout time.

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

For more information about the Junos Space Network Management Platform user interface, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

Related Documentation

- [Logging In to Junos Space on page 3](#)

PART 2

Devices

- [Device Management Overview on page 11](#)
- [Device Configuration on page 21](#)
- [Device Inventory on page 41](#)
- [Device Operations on page 67](#)
- [Device Access on page 85](#)
- [Device Monitoring on page 97](#)
- [Custom Attributes on page 103](#)
- [Discover Devices on page 109](#)
- [Model Devices on page 117](#)
- [Unmanaged Devices on page 133](#)
- [Secure Console on page 137](#)
- [Device Adapter on page 145](#)
- [Upload Keys to Devices on page 149](#)
- [Device Statistics on page 155](#)
- [QuickView on page 157](#)
- [Configuration Guides on page 159](#)

CHAPTER 2

Device Management Overview

- [Device Management Overview on page 11](#)
- [Device Inventory Overview on page 12](#)
- [Viewing Managed Devices on page 14](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Troubleshooting Devices on page 19](#)

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 133](#)

From the Devices workspace, you use the device discovery task 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 multiple 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.
- Reboot Devices.
- Troubleshoot devices.

Related Documentation

- [Device Discovery Overview on page 109](#)
- [Device Inventory Overview on page 12](#)
- [Managing DMI Schemas Overview on page 804](#)
- [Discovering Devices on page 111](#)
- [Systems of Record in Junos Space Overview on page 825](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Exporting License Inventory on page 47](#)

Device Inventory Overview

You manage the device inventory from the Devices workspace. 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 resynchronization 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.

You can use the device inventory to perform the following tasks:

- List the device inventory to view information about the hardware and software components of each device that Junos Space Network Management Platform 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 the credentials for devices.
- View the 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 devices.
- If the network is the system of record, resynchronize the network devices managed by Junos Space Network Management Platform.

**Related
Documentation**

- [Device Management Overview on page 11](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Viewing Physical Inventory on page 41](#)
- [Exporting Physical Inventory Information on page 53](#)
- [Exporting License Inventory on page 47](#)

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 399). If the network is the system of reference, the Network Monitoring workspace also enables you to resynchronize your managed devices (see “[Resyncing Nodes](#)” on page 400).

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 825.

To view configuration and run-time information for devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**. The Device Management page is displayed.

The following [Figure 1 on page 14](#) shows the Device Management page.

Figure 1: Device Management Page

Name	Physical Inter...	Logical Inter...	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 4 LSYS(a)	View	View	12.1X44-D10.4	junos-es	SRX1400	10.205.56.3	up	In Sync	---	---
10.205.56.4 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-es4500	View	View	11.3R7	junos-ex	EX4500-40F	10.155.69.77	up	Out Of Sync	---	---
delaware-es4500	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 9 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 3 on page 15](#) describes the fields displayed in the inventory window. In the table, an asterisk indicates that this column is not shown by default.

Table 3: 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.)
Configuration State	<p>The current state of the device configuration.</p> <ul style="list-style-type: none"> • NA - there is no change made to the configuration. This is the default state. • Created - When a change is made to the device configuration from Junos Space Network Management Platform. • Approved - Device configuration is approved. • Rejected - Device configuration is rejected.
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.)
Last Rebooted Time	The date and time when the device was last rebooted either manually (device status changes from DOWN to UP) or from Junos Space Network Management Platform.
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 804 .
IP Address	IP address of the device.
Connection Status	<p>Connection status of the device in Junos Space Network Management Platform. 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 3: 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-resynchronization 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 resynchronization 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.
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.)

- 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**.
- Show columns not in the default tabular view, or hide columns, as follows:
 - Mouse over any column header and click the down arrow.
 - Select **Columns** from the menu.
 - Select the check boxes for columns that you want to view. Clear the check boxes for columns that you want to hide.
- 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.

**Related
Documentation**

- [Viewing Physical Inventory on page 41](#)
- [Exporting License Inventory on page 47](#)
- [Viewing Physical Interfaces on page 44](#)
- [Discovering Devices on page 111](#)
- [Viewing the Node List on page 399](#)
- [Resyncing Nodes on page 400](#)
- [Systems of Record in Junos Space Overview on page 825](#)

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 17](#)
- [Junos Space as System of Record on page 19](#)

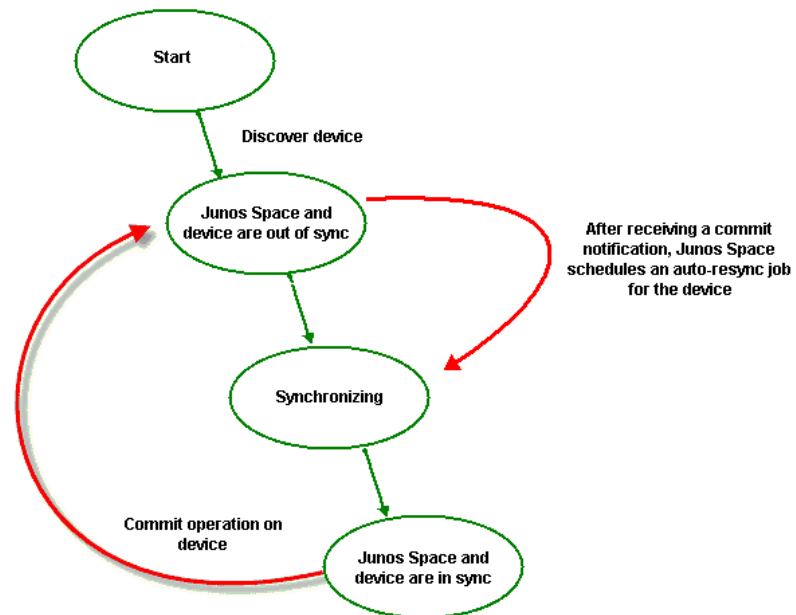
Network as System of Record

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-resynchronization 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 2 on page 18](#) shows how a commit operation on the device triggers resynchronization.

Figure 2: Resynchronization Process



When a commit operation is performed on a managed device under NSOR, Junos Space Network Management Platform, by default, schedules a resynchronization 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 resynchronization 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 resynchronization 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 resynchronization 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 resynchronization job begins on the device, the Managed Status for the device displays "Synchronizing" and then "In

Sync” after the resynchronization job has completed, unless a pending device commit operation causes the device to display “Out of Sync” while it was synchronizing.

When a resynchronization job is scheduled to run but another resynchronization job on the same device is in progress, Junos Space Network Management Platform delays the scheduled resynchronization 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 resynchronization job to the same device is in progress. When the currently running job finishes, the scheduled resynchronization job starts.

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

For information about setting the damper interval to change the resynchronization time delay and information about disabling the auto-resynchronization feature, see [“Modifying Junos Space Application Settings” on page 709](#).

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 825](#)
- [Device Discovery Overview on page 109](#)
- [Device Inventory Overview on page 12](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)

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 69](#).

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](#)

CHAPTER 3

Device Configuration

- [Modifying the Configuration on the Device on page 21](#)
- [Reviewing and Deploying the Device Configuration on page 25](#)
- [Viewing the Configuration Change Log on page 31](#)
- [Resolving Out of band Changes on page 32](#)
- [Filtering Devices by CSV on page 34](#)
- [Creating a Quick Template from the Device Configuration on page 34](#)
- [Viewing Assigned Shared Objects on page 35](#)
- [Viewing Template Deployment \(Devices\) on page 37](#)
- [Viewing Active Configuration on page 39](#)
- [Viewing Device Statistics on page 40](#)

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 the device configuration:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.
The Device Management page is displayed.
2. Right-click the device whose configuration you want to modify and select **Device Configuration > Modify Configuration**.
The **Modify Configuration** page is displayed.
3. You can use the schema-based configuration editor or configuration guides to modify the device configuration.
To use the schema-based configuration editor:
 - a. Select the **Schema-based Configuration Editor** to modify the configuration using the schema-based editor.
 - b. 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 173](#).

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

- c. Select **View/Configure** until you arrive at the parameter that you want to change.
- d. 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.

- e. (Optional) For information about individual parameters, click the little blue information icons to the right of the configuration settings to display the explanations.
- f. (Optional) To add comments about individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.
- g. (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.

- h. (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)**.

To modify the device configuration using the configuration guides:

- a. Select the **Basic Setup** link.

The Basic Setup pop-up window is displayed.

- b. (Optional) In the **Hostname** field, enter the hostname of the device.
- c. (Optional) In the **Domain name** field, enter the domain name of the device.
- d. (Optional) In the **Timezone** field, enter the hostname of the device.
- e. (Optional) Select the **Allow FTP file transfers** check-box if you want to allow FTP file transfers on the device.
- f. (Optional) Select the **Allow ssh access** check-box if you want to allow accessing the device using SSH.
- g. (Optional) Select the **Allow telnet login** check-box if you want to allow logging into the device using Telnet.
- h. In the NTP Server section, click the Add NTP Server icon to add an NTP server to the device.

The Add pop-up window is displayed. Enter the following details in this pop-up window.

- a. In the **Name** field, enter the name of the NTP server.
- b. (Optional) In the **Key** field, enter a value for the key.
- c. (Optional) From the **Version** drop-down list, select the appropriate version.
- d. (Optional) Select the **Prefer** check-box is required.
- e. Click **Create**.

Use the Edit NTP Server and Delete NTP Server icons to edit and modify the NTP server details respectively.

- i. In the User Management section, click the Add User icon to add users for the device.

The Add pop-up window is displayed. Enter the following details in this pop-up window.

- a. In the **Name** field, enter the name of the user.
- b. (Optional) Select an appropriate user ID from the **User ID** field.
The minimum value for this field is 100.
- c. (Optional) In the **Full Name** field, enter the full name of the user.
- d. (Optional) In the **Password** field, enter the password for the user.
- e. (Optional) In the **Re-enter Password** field, re-enter the password for the user.
- f. From the **Login Class** drop-down list, select the appropriate login class for the user.

The available login classes are super-user, operator, read-only, unauthorized, and wheel.

- g. Click **Create**.

Use the Edit User and Delete User icons to edit and modify the details of the user respectively.

- j. In the DNS Server section, click the DNS NTP Server icon to add a DNS server to the device.

The Add pop-up window is displayed. Enter the following details in this pop-up window.

- a. In the **Name** field, enter the name of the DNS server.
- b. Click **Create**.

Use the Edit DNS Server and Delete DNS Server icons to edit and modify the DNS server details respectively.

- k. Enter the following details in the SNMP section:

1. In the **Location** field, enter the location for SNMP..
2. Click the Add SNMP Community icon.

The Add pop-up window is displayed. Enter the following details in the Community section:

- a. In the **Name** field, enter the name of the SNMP community.
- b. (Optional) From the **Authorization** drop-down list, select the appropriate type of authorization.
- c. Click **Create**.

Use the Edit SNMP Community and Delete SNMP Community icons to edit and modify the SNMP Community details respectively.

3. Click the Add Trap Group icon.

The Add pop-up window is displayed. Enter the following details in the Trap Group section:

- a. In the **Name** field, enter the name of the trap group.

- b. (Optional) Select the check-box next to the appropriate trap group category.
- c. Click **Create**.

Use the Edit Trap Group and Delete Trap Group icons to edit and modify the trap group details respectively.

- l. Click **OK**.



NOTE: If you have installed the Security Director application on your Junos Space Network Management Platform setup and are modifying the configuration on an SRX Series device, you can use the additional Configuration Guides available on the Modify Configuration page. In this case, the Modify Configuration page lists the Configuration Guides to setup routing and security parameters on an SRX Series device. For more information on using the Configuration Guides related to routing and security parameters on an SRX Series device, see the Junos Space Security Director Application Guide.

- 4. You can either preview, save, or deploy the device configuration.
 - To preview the configuration before deploying it to the device, click **Preview**.
 - To save the configuration, click **Save**.
 - To deploy the configuration on the device, click **Deploy**.

Related Documentation

- [Device Management Overview on page 11](#)

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 35) 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 Configuration Changes on the Device on page 26](#)
- [Validating the Configuration on the Device on page 27](#)
- [View the Device-Configuration Validation Report on page 28](#)
- [Excluding or Including a Group of Configuration Changes on page 28](#)
- [Deleting a Group of Configuration Changes on page 29](#)
- [Approving the Configuration Changes on page 29](#)
- [Rejecting the Configuration Changes on page 30](#)
- [Deploying the Configuration Changes on page 30](#)

Viewing the Configuration Changes on the Device

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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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 4 on page 26](#) show the columns displayed in the Select Devices section.

Table 4: 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 5 on page 27](#) lists the tabs.

Table 5: Tabs to View Configuration Deltas

Tab 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
The Device Management page appears.
2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Right-click the device whose configuration you have modified and want to deploy and select **Device Configuration > 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.



NOTE: You can view the rejected configuration in the Change Summary tab.

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. On the Junos Space Network Management Platform user interface, select **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 13.3 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.



NOTE: You can check whether the configuration changes were deployed on a device, from the Job Details page. To go to the Job Details page, double-click the ID of the deployment job on the Job Management page. The Description column on this page specifies whether the configuration changes were deployed on the device. If the configuration changes were not deployed on the device, the column lists the reason for failure.

**Related
Documentation**

- [Device Management Overview on page 11](#)
- [Viewing Assigned Shared Objects on page 35](#)

Viewing the Configuration Change Log

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.

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 configuration change log:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
The Device Management 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 6 on page 32](#) describes its contents.

Table 6: Configuration Change Log

Column Name	Description
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 and 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.
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.

Related Documentation • [Resolving Out of band Changes on page 32](#)

Resolving Out of band Changes

You can resolve the Out-of-band changes and either accept or reject the configuration changes.

To resolve the out of band changes:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.
The Device Management page is displayed.
2. Select the device whose out-of-band configuration changes you want to resolve.
3. Select **Device Configuration > Resolve Out-of-band Changes** from the Actions menu.

The Resolve Out-of-band Changes page is displayed. [Table 7 on page 32](#) describes the columns on this page.

Table 7: Resolving Out-of-Band Changes

Column Name	Description
ID	ID of the configuration change entry
changeXML	The list of out-of-band changes in XML format
device ID	ID of the device

Table 7: Resolving Out-of-Band Changes (*continued*)

Column Name	Description
Device Name	Name of the device
Timestamp	The date and time at which the configuration change was made
Author	The user ID of the person who made the change. For out-of-band change, this is the credential used to log into the device CLI management interface.
Configuration Change	A link to the out-of-band changes in XML format
Action	Option buttons enabling you to select Accept or Reject

4. (Optional) To view the out-of-band change:
 - a. Click the **View** link in the appropriate row.
The Out-of-band Change XML pop-up window displays the out-of-band changes in XML format.
 - b. Click **OK** to close the pop-up window.
5. You can accept or reject individual changes or accept all the out-of-band changes.
 - To approve or reject individual out-of-band changes:
 - i. Select **Accept** or **Reject** in the appropriate row.
 - ii. Click **Submit**.
The Job Information dialog box is displayed with the job ID.
 - iii. Click **OK**.
You are redirected to the Device Management page.
 - To approve all the out-of-band changes:
 - i. Click **Accept All**.
 - ii. Click **Submit**.
The Job Information dialog box is displayed with the job ID.
 - iii. Click **OK**.
You are redirected to the Device Management page.

Related Documentation • [Viewing the Configuration Change Log on page 31](#)

Filtering Devices by CSV

You can filter the devices on the Device Management page using a CSV file.

To filter devices using a CSV file:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select **Filter by CSV** from the Actions menu.

The Select CSV File pop-up window is displayed.

3. Click **Browse** and select the CSV file from the local computer.

4. Click **Import**.

A progress bar is displayed. Junos Space Network Management Platform validates the values you provided in the CSV file. If the validation fails, a pop-window is displayed. This pop-up window displays the list of devices that were not validated.

If the CSV file is imported successfully, the Device Management page is filtered and lists only those devices whose host names were listed in the CSV file.

Related Documentation

- [Device Management Overview on page 11](#)

Creating a Quick Template from the Device Configuration

You create a quick template from a device configuration when you want to push this configuration to multiple devices by deploying the quick template. You create a quick template from a device configuration from the Devices workspace.

To create a quick template from the device configuration:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device whose configuration you want to migrate to a quick template and select **Device Configuration > Create Template from Device Configuration** from the contextual menu.

You are redirected to the Create Quick Template page in the Device Templates workspace. You can modify the Name field, and add or modify the device configuration using the CLI-based or Form-based editor.

3. Use the Create Quick Template workflow to create a quick template from the device configuration. For more information, see [“Creating a Quick Template” on page 206](#).

- Related Documentation**
- [Deploying a Quick Template on page 210](#)
 - [Quick Templates Overview on page 205](#)

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. On the Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

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

The View/Assign Shared Objects page is displayed. It lists 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 8 on page 36](#).

Table 8: View Assigned Shared Objects Table

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

3. To assign a template:

- a. 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.

- b. Select the check box for the configuration you want to assign, and click the [+] sign.

The template is assigned.

4. To unassign a template:

- a. 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.

- b. 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.

- c. Click **Yes** to dismiss the dialog.

The template disappears from the table.

5. To change the sequence of objects, assigned or otherwise:

- a. 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.

- b. (Optional) Continue moving objects the same way until you are satisfied.
6. Click **Save Changes** or **Save & Publish Changes**.

**Related
Documentation**

- [Modifying the Configuration on the Device on page 21](#)

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. On the Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page lists all the devices.

2. Select the device and select **Device Configuration > 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.

Column Header	Description
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.

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

The Template Details window appears.

- 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.

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

The Job Management window appears.

- 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 a Device Template Configuration” on page 202](#)).



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 a Device Template Configuration” on page 202](#).

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.

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

Related Documentation

- [Deploying a Template on page 195](#)

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. On the Network Management Platform user interface, select **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.

Related Documentation

- [Viewing Managed Devices on page 14](#)

Viewing Device Statistics

You can view the device statistics when you select the Devices workspace. The charts presented on the Devices landing page display the status of the device, and number of devices per OS and number of devices per platform. All the charts are interactive.

The Devices landing page displays the following charts related to 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 the device statistics:

1. On the Junos Space Network Management Platform user interface, select **Devices**.

The Devices landing page is displayed. This page displays the charts related to devices.

2. Click on any of the charts.

You will be redirected to the Devices page.

3. Click the specific label on a chart.

You will be redirected to the Devices page that is filtered based on the label you clicked.

Related Documentation

- [Viewing Managed Devices on page 14](#)
- [Viewing Physical Inventory on page 41](#)
- [Discovering Devices on page 111](#)

CHAPTER 4

Device Inventory

- [Viewing Physical Inventory on page 41](#)
- [Displaying Service Contract and EOL Data in the Physical Inventory Table on page 43](#)
- [Viewing Physical Interfaces on page 44](#)
- [Viewing Logical Interfaces on page 45](#)
- [Exporting License Inventory on page 47](#)
- [Viewing and Exporting Software Inventory on page 51](#)
- [Exporting Physical Inventory Information on page 53](#)
- [Viewing Associated Scripts on page 54](#)
- [Executing a Promoted Script on a Device on page 54](#)
- [Executing Scripts on a Physical Inventory Component on page 56](#)
- [Executing a Promoted Script on a Physical Inventory on page 57](#)
- [Executing Scripts on a Physical Interface on page 58](#)
- [Executing a Promoted Script on a Physical Interface on page 59](#)
- [Executing Scripts on a Logical Interface on page 60](#)
- [Executing a Promoted Script on a Logical Interface on page 61](#)
- [Applying CLI Configlets to the Physical Inventory on page 62](#)
- [Applying CLI Configlets to Physical Interfaces on page 63](#)
- [Applying CLI Configlets to Logical Interfaces on page 64](#)
- [Viewing Staged Images on a Device on page 64](#)
- [Deleting Staged Images on a Device on page 65](#)

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 resynchronization 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. On the Network Management Platform user interface, 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. You can also view the name of the device in the Device Name column and the domain to which the device belongs in the Domain column of the table.

The Status field on the Physical Inventory page displays the status of the device component. The status is updated during the periodic re-synchronization and on notification. The different status indicators are Online and Offline.

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 43](#) [“Displaying Service Contract and EOL Data in the Physical Inventory Table” on page 43](#).

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 53](#).
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 43](#)
- [Exporting Physical Inventory Information on page 53](#)
- [Viewing Managed Devices on page 14](#)
- [Viewing Physical Interfaces on page 44](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Exporting License Inventory on page 47](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)

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 41](#)

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 enabled for the physical interfaces view. 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 Devices Management page, or from within the Physical Inventory page.

To view the physical interfaces for devices from the Device Management page:

1. On the Network Management Platform user interface, 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 9 on page 44](#) 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 9: Physical Interfaces Columns

Column	Description
Device Name	Configuration name of the device. This column is displayed by default.
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	IP address for the interface
Logical Interfaces	Link to the table of logical interfaces for the device
MAC Address	MAC address of the device
Operational Status	Operational status of the interface: up or down
Admin Status	Admin status of the interface: up or down
Link Level Type	Link level type of the physical interface

Table 9: Physical Interfaces Columns (*continued*)

Column	Description
Link Type	Physical interface link type: full duplex or half duplex
Speed (Mbps)	Speed at which the interface is running
MTU	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.
Domain	Domain to which the device is assigned

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 9 on page 44](#) 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 14](#)
- [Viewing Physical Inventory on page 41](#)
- [Exporting License Inventory on page 47](#)
- [Viewing Logical Interfaces on page 45](#)

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. On the Network Management Platform user interface, select **Devices > Device Management**.
A tabular list of devices appears.
2. Select the device for which you want to view logical interface information and select **Device Inventory > View Logical Interfaces** from the Actions menu.

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 10 on page 46](#). 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 10: Logical Interfaces Columns

Column	Description
Device Name	Configuration name of the device. This column is displayed by default.
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	IP address for the logical interface
Encapsulation	Encapsulation type used on the logical interface
Vlan	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.
Domain	Domain to which the device is assigned

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

Related Documentation

- [Viewing Physical Interfaces on page 44](#)

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 703](#).

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 825](#).

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 68](#).

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. 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 export the license inventory for a device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

The Device Management 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 11 on page 49](#).



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 12 on page 50](#).

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 12 on page 50](#) and [Table 13 on page 50](#). 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 11: 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.

Table 11: License Usage Summary Fields (*continued*)

Field	Description
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.
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 12: 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 13: 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 14](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Systems of Record in Junos Space Overview on page 825](#)

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 825](#).

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 68](#).

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.

You can export device software inventory information to a CSV file for use in other applications (steps 5 through 7).

To export the software inventory for a device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

The Device Management 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 list, 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 14 on page 52](#), 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 14: Software Inventory Fields

Field	Description
Device Name	Name of the device on which this software inventory is present
Model	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	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 14](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Systems of Record in Junos Space Overview on page 825](#)
- [Device Images and Scripts Overview on page 265](#)

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. On the Network Management Platform user interface, select **Devices > Device Management**.

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

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 12](#)
 - [Viewing Managed Devices on page 14](#)
 - [Viewing Physical Inventory on page 41](#)
 - [Device Management Overview on page 11](#)
 - [Device Discovery Overview on page 109](#)

Viewing Associated Scripts

You can view the scripts deployed on a device to get more information about the script type, version, and activation status.

To view the scripts associated with the devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

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

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 12](#)

Executing a Promoted Script on a Device

You execute a promoted script from the Devices workspace. You can execute a promoted script on a device, the physical interface of a device, the logical interface of a device, or the physical inventor of a device.

To execute a promoted script on a device:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device on which you want to execute the promoted script and select **Device Operations > Select the Promoted Script** from the Actions menu.

The Promoted script that appears satisfies the following criteria:

- It is associated and enabled on the selected device.
 - Advanced Xpath Processing in Junos Space Network Management Platform settings is enabled.
 - The context of the script matches the context of the selected device.
3. Enter the values for the parameters.
 4. (Optional) To schedule a time for Execution, select the Schedule at a later time check box and specify the date and time when the script has to be executed.
 5. Click **Execute**.

The Script Execution Job Results window is displayed.

The results page displays following information-Device name, Entity name, Script Execution status and Script Execution Results. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results. It also includes the progress bar indicating the status of Script Execution Job. If there is ONCLOSESTRING then the Result page will get closed automatically when the ONCLOSESTRING matches the script execution result string.



NOTE: When the Script Execution Job is scheduled, the Script Execution Job Results window does not appear, instead Job dialog box appears displaying a link to the Job ID. The user can click the link to view the status of this task on the Manage Jobs page. On double clicking the task, Script Management Job status window appears. The user can click on View Results link under Description column to view the results of Script Execution. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results.

Click **Cancel** to return to the Device Management page.

Related Documentation

- [Promoting Scripts Overview on page 279](#)

Executing Scripts on a Physical Inventory Component

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.

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

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Inventory > View Physical Inventory** from the Actions menu.

3. 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.

4. 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.

5. Enter the values for the parameters.

6. 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.

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 Job Management 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 62](#)

Executing a Promoted Script on a Physical Inventory

You execute a promoted script from the Devices workspace. You can execute a promoted script on a device, the physical interface of a device, the logical interface of a device, or the physical inventor of a device.

To execute a promoted script on a physical inventory component:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device with the physical inventory component on which you want to execute the promoted script and select **Device Inventory > View Physical Inventory** from the contextual menu.
3. Right-click the physical inventory component and select **Promoted Script** from the contextual menu.

The Promoted script that appears satisfies the following criteria:

- It is associated and enabled on the selected device.
 - Advanced Xpath Processing in Junos Space Network Management Platform settings is enabled.
 - The context of the script matches the context of the selected physical inventory component.
4. Enter the values for the parameters.
 5. (Optional) To schedule a time for Execution, select the Schedule at a later time check box and specify the date and time when the script has to be executed.
 6. Click **Execute**.

The Script Execution Job Results window is displayed.

The results page displays following information-Device name, Entity name, Script Execution status and Script Execution Results. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results. It also includes the progress bar indicating the status of Script Execution Job. If there is ONCLOSESTRING then the Result page will get closed automatically when the ONCLOSESTRING matches the script execution result string.



NOTE: When the Script Execution Job is scheduled, the Script Execution Job Results window does not appear, instead Job dialog box appears displaying a link to the Job ID. The user can click the link to view the status of this task on the Manage Jobs page. On double clicking the task, Script Management Job status window appears. The user can click on View Results link under Description column to view the results of Script Execution. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results.

Click **Cancel** to return to the View Physical Inventory page.

Related Documentation

- [Promoting Scripts Overview on page 279](#)

Executing Scripts on a Physical Interface

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.

To execute scripts on a physical interface of the device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Inventory > > View Physical Interfaces**.
3. 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.

4. 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.

5. Enter the values for the parameters.
6. 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.
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 Job Management 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 Devices on page 77](#)

Executing a Promoted Script on a Physical Interface

You execute a promoted script from the Devices workspace. You can execute a promoted script on a device, the physical interface of a device, the logical interface of a device, or the physical inventor of a device.

To execute a promoted script on a physical interface:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device with the physical interface on which you want to execute the promoted script and select **Device Inventory > View Physical Interfaces** from the contextual menu.
3. Right-click the physical interface and select **Promoted Script** from the contextual menu.

The Promoted script that appears satisfies the following criteria:

- It is associated and enabled on the selected device.
 - Advanced Xpath Processing in Junos Space Network Management Platform settings is enabled.
 - The context of the script matches the context of the selected physical interface.
4. Enter the values for the parameters.
 5. (Optional) To schedule a time for Execution, select the Schedule at a later time check box and specify the date and time when the script has to be executed.
 6. Click **Execute**.

The Script Execution Job Results window is displayed.

The results page displays following information-Device name, Entity name, Script Execution status and Script Execution Results. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results. It also includes the progress bar indicating the status of Script Execution Job. If there is ONCLOSESTRING then the Result page will get closed automatically when the ONCLOSESTRING matches the script execution result string.



NOTE: When the Script Execution Job is scheduled, the Script Execution Job Results window does not appear, instead Job dialog box appears displaying a link to the Job ID. The user can click the link to view the status of this task on the Manage Jobs page. On double clicking the task, Script Management Job status window appears. The user can click on View Results link under Description column to view the results of Script Execution. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results.

Click **Cancel** to return to the View Physical Interface page.

Related Documentation

- [Promoting Scripts Overview on page 279](#)

Executing Scripts on a Logical Interface

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.

To execute scripts on a logical interface of the device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Inventory > > View Physical Interfaces** from the Actions menu.
3. 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.

4. 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.

5. Enter the values for the parameters.

6. 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.
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 Job Management 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 Devices on page 77](#)

Executing a Promoted Script on a Logical Interface

You execute a promoted script from the Devices workspace. You can execute a promoted script on a device, the physical interface of a device, the logical interface of a device, or the physical inventor of a device.

To execute a promoted script on a logical interface:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device with the logical interface on which you want to execute the promoted script and select **Device Inventory > View Logical Interfaces** from the contextual menu.
3. Right-click the logical interface and select **Promoted Script** from the contextual menu.

The Promoted script that appears satisfies the following criteria:

- It is associated and enabled on the selected device.
 - Advanced Xpath Processing in Junos Space Network Management Platform settings is enabled.
 - The context of the script matches the context of the selected logical interface.
4. Enter the values for the parameters.

5. (Optional) To schedule a time for Execution, select the Schedule at a later time check box and specify the date and time when the script has to be executed.
6. Click **Execute**.

The Script Execution Job Results window is displayed.

The results page displays following information-Device name, Entity name, Script Execution status and Script Execution Results. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results. It also includes the progress bar indicating the status of Script Execution Job. If there is ONCLOSESTRING then the Result page will get closed automatically when the ONCLOSESTRING matches the script execution result string.



NOTE: When the Script Execution Job is scheduled, the Script Execution Job Results window does not appear, instead Job dialog box appears displaying a link to the Job ID. The user can click the link to view the status of this task on the Manage Jobs page. On double clicking the task, Script Management Job status window appears. The user can click on View Results link under Description column to view the results of Script Execution. Here the result HTML is processed and rendered, thus enabling the user to easily read and understand the Script Execution Results.

Click **Cancel** to return to the View Logical Interface page.

Related Documentation

- [Promoting Scripts Overview on page 279](#)

Applying CLI Configlets to the Physical Inventory

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. You apply a CLI configlet to push a configuration to the devices.

To apply a CLI configlet to the physical inventory of a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
- The Device Management page is displayed.
2. Right-click the device and select **Device Inventory > View Physical Inventory** from the Actions menu.
 3. Right-click the physical inventory element for which you want to apply the CLI configlet.
 4. 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.

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

- Related Documentation**
- [CLI Configlets Workflow on page 216](#)
 - [CLI Configlets Overview on page 215](#)

Applying CLI Configlets to Physical Interfaces

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. You apply a CLI configlet to push a configuration to the devices.

To apply a CLI configlet to the physical interfaces of a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Inventory > View Physical Interfaces** from the Actions menu.
3. Right-click the physical interfaces for which the CLI configlet has to be applied.
4. Select **Apply CLI Configlets**.

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

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

- Related Documentation**
- [CLI Configlets Workflow on page 216](#)
 - [CLI Configlets Overview on page 215](#)

Applying CLI Configlets to Logical Interfaces

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. You apply a CLI configlet to push a configuration to the devices.

To apply a CLI configlet to the logical interfaces of a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Inventory > View Logical Interfaces** from the Actions menu.
3. Right-click the logical interfaces for which the CLI configlet has to be applied
4. Select **Apply CLI Configlets**.

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

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

- Related Documentation**
- [CLI Configlets Workflow on page 216](#)
 - [CLI Configlets Overview on page 215](#)

Viewing Staged Images on a Device

You can view images staged on a device from the Device Management page. You can also verify the checksum from this page. Currently, you cannot view the images staged on an LSYS type device by using this workflow.

To view the images staged on a device:

1. From the Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Select the device for which you want to view the staged images and select **Device Inventory > View Staged Images** from the Actions menu.

The View Staged Images page is displayed. [Table 15 on page 65](#) describes the columns displayed on this page.

Table 15: View Staged Images Page

Column Name	Description
Device Name	Name of the device
Image Name	Name of the device image
IP Address	IP address of the device
Platform	Platform to which the device belongs
Checksum Status	Whether the device image on the Junos Space server and the device are the same: <ul style="list-style-type: none"> • If the status is Valid, the checksum values of the device image on the Junos Space server and the device match. • If the status is Invalid, the checksum values do not match. • If the status is NA, the selected image is not staged on the device yet.
Last Checksum Time	Time when the checksum was last verified For a device on which the selected image is not staged yet, this column displays NA.

3. After you view the image staged on the device, click **Back** at the top of the View Staged Images page to return to the Device Management page.



NOTE: You can select multiple devices on the Device Management page to view the images staged on these devices. Click the '+' symbol next to the device to view the images staged on the device. The View Staged Images page lists only the devices on which the images are staged. If you select a device that does not have staged images, this device is not displayed on the View Staged Images page.

Related Documentation

- [Device Images Overview on page 273](#)
- [Staging Device Images on page 286](#)
- [Deleting Staged Images on a Device on page 65](#)

Deleting Staged Images on a Device

You can delete images staged on a device from the Device Management page. Currently, you cannot delete the images staged on an LSYS type device by using this workflow..

To delete the images staged on a device:

1. From the Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

The Device Management page is displayed.

2. Select the device from which you want to delete the staged images and select **Device Inventory > View Staged Images** from the Actions menu.

The View Staged Images page is displayed.

3. Select the staged images that you want to delete from the device.
4. Click the Delete Images icon on the Actions menu.

A job is created. You can view the status of the job on the Job Management page.

5. After you delete the staged images on a device, click **Back** at the top of the View Staged Devices page to return to the Device Management page.



NOTE: You can select multiple devices on the Device Management page to delete the images staged on these devices. Click the “+” symbol next to the each device, select the staged images, and click the Delete Images icon on the Actions menu. The View Staged Images page lists only the devices on which the images are staged. If you select a device that does not have staged images, this device is not displayed on the View Staged Images page.

**Related
Documentation**

- [Device Images Overview on page 273](#)
- [Staging Device Images on page 286](#)
- [Viewing Staged Images on a Device on page 64](#)

CHAPTER 5

Device Operations

- [Deleting Devices on page 67](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Using Looking Glass on page 69](#)
- [Understanding Logical Systems for SRX Series Services Gateways on page 71](#)
- [Creating a Logical System \(LSYS\) on page 71](#)
- [Deleting Logical Systems on page 72](#)
- [Viewing the Physical Device for a Logical System on page 73](#)
- [Viewing Logical Systems for a Physical Device on page 74](#)
- [Putting a Device in RMA State and Reactivating Its Replacement on page 75](#)
- [Applying CLI Configlets to Devices on page 76](#)
- [Executing Scripts on Devices on page 77](#)
- [Executing Scripts on Devices Locally with JUISE on page 78](#)
- [Modifying the Serial Number of a Device on page 80](#)
- [Rebooting Devices on page 81](#)
- [Creating Device Partitions on page 82](#)
- [Deleting Device Partitions on page 83](#)
- [Modifying Device Partitions on page 83](#)

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.

If provisioning services are associated with a device that you want to delete, you must remove the provisioning services before deleting the device.

To delete devices:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Select the devices you want to delete and select **Device Operations > Delete Devices** from the Actions menu.

The Delete Devices pop-up window is displayed.

3. Click **Confirm**.

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 14](#)
- [Viewing Physical Inventory on page 41](#)
- [Viewing Physical Interfaces on page 44](#)
- [Discovering Devices on page 111](#)

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 825.)

To resynchronize a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Select the devices you want to resynchronize and select **Device Operations > Resynchronize with Network** from the Actions menu.

The Resynchronize Devices pop-up window is displayed.

3. Click **Confirm**.

When a resynchronization job is scheduled to run but another resynchronization job on the same device is in progress, Junos Space Network Management Platform delays the scheduled resynchronization 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 resynchronization job to the same device is in progress. When the job that is currently running finishes, the scheduled resynchronization job starts. See “[Modifying Junos Space Application Settings](#)” on page 709.



NOTE: You can check whether a managed device was resynchronized with the network, from the Job Details page. To go to the Job Details page, double-click the ID of the resynchronization job on the Job Management page. The Description column on this page specifies whether the managed device was resynchronized with the network. If the managed device was not resynchronized with the network, the column lists the reason for failure.

Related Documentation

- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Systems of Record in Junos Space Overview on page 825](#)
- [Device Inventory Overview on page 12](#)
- [Viewing Physical Inventory on page 41](#)
- [Viewing Physical Interfaces on page 44](#)
- [Exporting License Inventory on page 47](#)

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 tabular view. Text output simulates the CLI, whereas tabular 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 logical systems.

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

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
The Device Management page appears.
2. Select the device you want to run the **show** command for and 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 tabular 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**

- [Discovering Devices on page 111](#)
- [Viewing Managed Devices on page 14](#)
- [Viewing Physical Inventory on page 41](#)
- [Viewing Physical Interfaces on page 44](#)

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 the Physical Device for a Logical System on page 73](#)
- [Viewing Logical Systems for a Physical Device on page 74](#)
- [Creating a Logical System \(LSYS\) on page 71](#)
- [Deleting Logical Systems on page 72](#)

Creating a Logical System (LSYS)

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.



NOTE: You must create a LSYS profile on the device before creating a logical system. To create a LSYS profile on a device from Junos Space Platform, deploy the configuration to create a LSYS profile by using Junos Space Platform features such as device templates or CLI Configlets. To create a LSYS profile by using the Quick Templates feature, see [“Creating a Quick Template” on page 206](#) and [“Deploying a Quick Template” on page 210](#).

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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. Select a device for which you want to create a logical system and then select **Device Operations > Create LSYS** from the Actions menu.

The New Logical System pop-up window is displayed.

3. In the **LSYS device name** field, enter a user-defined name for the new logical system.
4. From the **LSYS profile** drop-down list, choose a logical system security profile for the new logical system.



NOTE: If you have not created a LSYS profile on the device, the drop-down list will not display any LSYS profiles.

5. Click **Finish** to create the new logical system.

Related Documentation

- [Understanding Logical Systems for SRX Series Services Gateways on page 71](#)
- [Viewing Devices and Logical Systems with QuickView on page 157](#)
- [Viewing the Physical Device for a Logical System on page 73](#)
- [Viewing Logical Systems for a Physical Device on page 74](#)
- [Deleting Logical Systems on page 72](#)
- *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 logical systems:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
The Device Management page is displayed.
2. Select a logical system and select **Device Operations > Delete Devices** from the Actions menu.
The Delete Logical Systems pop-up window is displayed.
3. Click **Confirm** to proceed with the deletion of the logical systems.

Related Documentation

- [Understanding Logical Systems for SRX Series Services Gateways on page 71](#)
- [Viewing Devices and Logical Systems with QuickView on page 157](#)
- [Viewing the Physical Device for a Logical System on page 73](#)
- [Viewing Logical Systems for a Physical Device on page 74](#)
- [Creating a Logical System \(LSYS\) on page 71](#)
- *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. On the Network Management Platform user interface, select **Devices > Device Management**.
The Device Management page displays the devices managed in Junos Space Network Management Platform.
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 71](#)
- [Viewing Devices and Logical Systems with QuickView on page 157](#)
- [Viewing Logical Systems for a Physical Device on page 74](#)
- [Creating a Logical System \(LSYS\) on page 71](#)
- [Deleting Logical Systems on page 72](#)
- *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. On the Network Management Platform user interface, select **Devices > Device Management**.

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

3. 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)."

4. 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.

5. 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 71](#)
- [Viewing Devices and Logical Systems with QuickView on page 157](#)
- [Viewing the Physical Device for a Logical System on page 73](#)
- [Creating a Logical System \(LSYS\) on page 71](#)
- [Deleting Logical Systems on page 72](#)

- *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 75](#)
- [Reactivating a Replacement Device on page 76](#)

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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
The Device Management page is displayed.
2. Select the defective device and select **Device Operations > Put in RMA State** from the Actions menu.

The RMA Device window appears.

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

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 reactivate the replacement device:

1. Connect the replacement device to your network in the same way as the defective device was connected.
2. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

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 replacement device is displayed with the defective device's configuration in the Device Management page. 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 Devices

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. You apply a CLI configlet to push a configuration to the devices.

To apply a CLI configlet to devices:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the devices and select **Device Operations > Apply CLI Configlet** from the Actions menu.

The Apply CLI Configlet page is displayed. It lists the CLI configlets that match the context of the selected devices.

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

- Related Documentation**
- [CLI Configlets Workflow on page 216](#)
 - [CLI Configlets Overview on page 215](#)

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.

To execute scripts on a selected device from the Devices workspace:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Operations > Execute Scripts** from the Actions menu.

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.

3. 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.

4. Enter the values for the parameters.
5. 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.
6. 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 Job Management 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 76](#)

Executing Scripts on Devices Locally with JUISE

The Junos Space image comes integrated with the Junos OS User Interface Scripting Environment (JUISE)—that is, juisse-0.3.10-1 version, which enables you to execute a script on a remote device from the Junos Space server without having to stage the script on the device. The conditions that should be met are:

- The device should be reachable from the Junos Space server
- The **@ISLOCAL** annotation marked within the script should be set to true. For example, the script should contain the following text:

```
/* @ISLOCAL = "true" */
```

When this annotation is set to false, you have to stage the script on a device first and then execute it. For more information about script annotations, see [“Scripts Annotations” on page 367](#).

From the Junos Space user interface, you can make out the scripts that can be executed locally from the **Execution Type** column by the **Local** value displayed in this column.

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

To execute scripts on Junos OS devices with JUISE:

1. On the Junos Space Network Management Platform user interface, select **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.



TIP: Identify and select only those scripts that have Local displayed in the **Execution Type** column.

3. Select **Execute Script on Devices** from the Actions menu.

The Execute Script on Device(s) page appears.

4. Select the devices on which you want the script to be executed, by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- 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; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

5. (Optional) To specify values for the parameters for script execution, click **Enter Parameter Value** for each parameter.
6. 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.
7. Click **Execute**.

The selected scripts are executed on the devices, and the Execute Script Information dialog box displays a link to the job ID. You can click the link to view the status of this task on the Job Management page. Double-click the task to view the Script Management Job status page. Click the **View Results** link in the **Description** column to view the results of script execution. The Script Execution Job Results page allows you to read and understand the Script Execution Results. Click the X icon to close this page.

You can export the details about the execution of a script as a comma separated values (CSV) file:

- a. Double-click the job pertaining to this execute operation.

The Script Management Job Status page appears.

- b. Click **Export as CSV**.

You are prompted to save the file.

- c. Click **OK** on the File Save dialog box to save the file to your local file system.

- d. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. Typically, you can view the script output on the Description column on this file.

- Related Documentation**
- [Scripts Overview on page 275](#)
 - [Executing Scripts on Devices on page 331](#)

Modifying the Serial Number of a Device

You modify the serial number of a device that is added to Junos Space Network Management Platform.

To modify the serial number of a modeled device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select the modeled device for which you want to modify the serial number and select **Device Operations > Modify Serial Number** from the Actions menu.

The Modify Serial Number page is displayed.

3. Double-click the serial number in the Serial Number column of the device and enter the new serial number.
4. Click **Modify**.

The serial number of the modeled device is modified.

Related Documentation

- [Model Devices Overview on page 117](#)
- [Creating a Modeled Instance on page 122](#)
- [Adding More Devices to an Existing Modeled Instance on page 126](#)
- [Downloading a Configlet on page 127](#)
- [Viewing and Copying Configlet Data on page 127](#)

Rebooting Devices

You can reboot devices from Junos Space Network Management Platform. You can also reboot virtual chassis setups, dual Routing Engine (RE) setups, and cluster setups from Junos Space Network Management Platform. You cannot reboot Logical System (LSYS) devices from Junos Space Network Management Platform.

To reboot devices:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select the devices that you want to reboot and select **Device Operations > Reboot Devices** from the Actions menu.

The Reboot Devices pop-up window is displayed. This pop-up window displays the devices that you selected for reboot and some additional options that you can configure before the reboot.

3. (Optional) Select the **Options** option button. Configure the following options in this section:
 - a. In the **Message** field, enter a message to indicate the purpose of this reboot operation.
 - b. Select the **Power off** option button.
4. (Optional) To schedule a time for reboot, select the **Schedule at a later time** option button and use the lists to specify the date and time.
5. Click **Confirm**.

The devices that you selected will be rebooted. A job will be created. You can view the job results from the Job Management page. If some of the devices fail to reboot, you can use the Retry on Failed Devices action to retry rebooting the devices that failed to reboot. For more information, see [“Retrying a Job on Failed Devices” on](#)

[page 511](#). When you reboot devices, an audit log entry is automatically generated. You can view the audit logs from the Audit Logs workspace.



NOTE: To reboot a single device, select only one device on the Device Management page and select **Device Operations > Reboot Devices** from the Actions menu.

**Related
Documentation**

- [Device Management Overview on page 11](#)
- [Viewing Managed Devices on page 14](#)

Creating Device Partitions

Create device partitions when you want to share the physical interfaces, logical interfaces, and physical inventory elements across multiple sub-domains. Device partitions are supported only on M Series and MX Series routers. You can partition a device from the Device Management workspace. You can assign only one partition from a device to a sub-domain; you cannot assign multiple partitions from the same device to a sub-domain. A maximum of one partition can be assigned from multiple devices to a sub-domain. You can partition a device only if the device is currently assigned to the global domain. For more information, see [“Working with Domains” on page 564](#).

To create a device partition:

1. On the Junos Space Network Management Platform user interface, select **Device > Device Management**.

The Device Management page is displayed.

2. Select the device that you want to partition and select **Device Operations > Manage Device Partitions** from the Actions menu.

The Manage Device Partitions page is displayed.

3. Click the Create Partition icon from the Actions menu.

The Create Partition page is displayed. You can view the physical interfaces, logical interfaces, and the physical inventory of the device.

4. In the **Partition Name** field, enter a name for the partition.

5. Select the **Physical Interface** tab and select the physical interfaces that you want to add to the partition.

You can view the selected physical interfaces in the Selected Sub-object section.

6. Select the **Logical Interface** tab and select the logical interfaces that you want to add to this partition.

You can view the selected logical interfaces in the Selected Sub-object section.

7. Select the **Physical Inventory** tab and select the inventory elements that you want to add to this partition.

You can view the selected inventory elements such as FPCs, and Routing Engines in the Selected Sub-object section.

8. Click **OK**.

The new device partition is created. Repeat steps 3 through 8 to add multiple device partitions. You can now assign this partition to a sub-domain.



NOTE: When you create the second device partition, the physical interfaces, logical interfaces, and physical inventory elements that you assigned to the first device partition are not available for selection.

Related Documentation

- [Modifying Device Partitions on page 83](#)

Deleting Device Partitions

You can delete the device partitions on a device from the Devices workspace. The device partitions are listed on the Device Management page.

To delete device partitions:

1. On the Junos Space Network Management Platform user interface, select **Device > Device Management**.

The Device Management page is displayed. You can view the devices and the device partitions on this page.

2. Select the device whose device partitions you want to delete and select **Device Operations > Manage Device Partitions** from the Actions menu.

The Manage Device Partitions page is displayed.

3. Select the device partitions that you want to delete and click the Delete Partition icon on the Actions menu.

The Delete Partition pop-up window is displayed.

4. Click **Delete**.

The device partitions are deleted.

Related Documentation

- [Managing Domains Overview on page 557](#)
- [Creating Device Partitions on page 82](#)
- [Modifying Device Partitions on page 83](#)

Modifying Device Partitions

You can modify device partitions from the Devices workspace. The device partitions are listed on the Device Management page.

To modify device partitions:

1. On the Junos Space Network Management Platform user interface, select **Device > Device Management**.

The Device Management page is displayed. You can view the devices and the device partitions on this page.

2. Select the device whose device partitions you want to modify and select **Device Operations > Manage Device Partitions** from the Actions menu.

The Manage Device Partitions page is displayed.

3. Select the device partition you want to modify and click the Modify Partition icon on the Actions menu.

The Modify Partition page is displayed.

4. Modify the physical interfaces, logical interfaces, and physical inventory elements for this device partition. You cannot modify the name of the partition.

5. Click **OK**.

6. Repeat steps 3 through 5 to modify any other device partitions.

The device partitions are modified.

**Related
Documentation**

- [Managing Domains Overview on page 557](#)
- [Creating Device Partitions on page 82](#)
- [Deleting Device Partitions on page 83](#)

CHAPTER 6

Device Access

- [Secure Console Overview on page 85](#)
- [Connecting to a Device From Secure Console on page 86](#)
- [Launching a Device's Web User Interface on page 90](#)
- [Key-Based Authentication Overview on page 91](#)
- [Generating and Uploading Authentication Keys to Devices on page 92](#)
- [Resolving Key Conflicts on page 95](#)
- [Changing Device Authentication from Password-based to Key-based Authentication on page 96](#)

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 86](#)

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 86](#)
- [Connecting to an Unmanaged Device from the Device Management Page on page 87](#)
- [Connecting to a Managed or Unmanaged Device from the Secure Console Page on page 89](#)

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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select a device to which you want to connect and select **Device Access > SSH to Device** from the Actions menu.

The SSH to Device pop-up window is displayed.



NOTE: If you have cleared the **Allow users to auto log in to devices using SSH** option on the **Modify Application Settings** page, the **SSH to Device** pop-up window is displayed. The IP address is automatically displayed in the IP address field. Enter the username and password in the **User name** and **Password** fields respectively.

3. In the **IP Address** field, enter a valid IP address of the device.

4. In the **Username** field, enter the user-name of the device.

The username must match the username configured on the device.

5. In the **Password** field, enter the password to access the device.

The password must match the password configured on the device.

6. 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.



NOTE: If you enter a port number other than the one you specified on the Modify Application Settings page, the SSH connection is not established.

7. Click **Connect**.

The SSH terminal window is displayed.



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

8. You can perform the following tasks in the terminal window:

- (Optional) Enter CLI commands to monitor and troubleshoot the device from this terminal window. Use the following terminal control characters:
 - **CRTL + A**—Moves cursor to the start of the command line
 - **CRTL + E**—Moves cursor to the end of the command line
 - **↑** (Up arrow key)—Repeats the previous command
 - **TAB**—Completes a partially typed command
- (Optional) Terminate a process by using the **CRTL + C** key combination.
- To terminate the SSH session, type **exit** and press Enter.

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.
- Clear the **Allow users to auto log in to devices using SSH** option on the Modify Application Settings page.

To connect to an unmanaged device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select a device to which you want to connect and select **Device Access > SSH to Device** from the Actions menu.

The SSH to Device pop-up window is displayed.

3. In the **IP Address** field, enter a valid IP address of the device.

4. In the **Username** field, enter the user-name of the device.

The username must match the username configured on the device.

5. In the **Password** field, enter the password to access the device.

The password must match the password configured on the device.

6. 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.



NOTE: If you enter a port number other than the one you specified on the Modify Application Settings page, the SSH connection is not established.

7. Click **Connect**.

The SSH terminal window is displayed.



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

8. You can perform the following tasks in the terminal window:
 - (Optional) Enter CLI commands to monitor and troubleshoot the device from this terminal window. Use the following terminal control characters:
 - **CRTL + A**—Moves cursor to the start of the command line
 - **CRTL + E**—Moves cursor to the end of the command line
 - **↑** (Up arrow key)—Repeats the previous command
 - **TAB**—Completes a partially typed command
 - (Optional) Terminate a process by using the **CRTL + C** key combination.
 - To terminate the SSH session, type **exit** and press Enter.

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 85](#)

Launching a Device's Web User Interface

The Launch Device Web UI 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Right-click the device and select **Device Access > Launch Device WebUI**.
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 14](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Managing Configuration Files Overview on page 473](#)

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 (which uses public-key cryptographic principles). 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 92. 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 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.

Junos Space Network Management Platform automates the 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 92](#)

Generating and Uploading Authentication Keys to Devices

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.

- [Generating Authentication Keys on page 92](#)
- [Uploading Authentication Keys to Multiple Managed Devices for the First Time on page 93](#)
- [Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space on page 94](#)

Generating Authentication Keys

To generate a public/private key pair for authentication during login to network devices:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.
The Fabric page is displayed.
2. Click the Generate Key icon on the Actions bar.
The Key Generator pop-up window is displayed.
3. (Optional) In the **Passphrase** field, enter a passphrase to be used to protect the private key, which remains on the system running Junos Space Network Management Platform and is used during device login. 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 impedes an attacker who may gain control of your system and try to log in to your managed network devices.
4. (Optional) Schedule the Junos Space Network Management Platform to generate authentication keys at a later time or immediately.
 - To specify a later start date and time for key generation, select the **Schedule at a later time** check box.
 - To initiate 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 the Junos Space server time but uses the local time zone of the client computer.

5. Click **Generate**.

The Generate Key Job Information dialog box appears, displaying a job ID link for key generation. Click the link to determine whether the key is generated successfully.

Uploading Authentication Keys to Multiple Managed Devices for the First Time

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Click the Upload Keys to Devices icon on the Actions bar.

The Upload Keys to Devices pop-up window is displayed.

3. To upload keys to a single device:

- a. Select **Add Manually**.

The Authentication Details field appears within the Upload Keys to Devices dialog box.

- b. Select **IP Address** or **Hostname**.

- c. In the **IP Address/Host Name** field, enter the IP address or the hostname of the target managed device.

- d. In the **Device Admin** field, enter the appropriate username for that device.

- e. In the **Password** field, 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, CSV file select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

The sample CSV contains the format for entering 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 the “user admin” user on the device.

- c. When 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 a .csv extension.
- e. Click **Upload** to upload the authentication 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 are uploaded and whether this operation is a success.

The green check mark adjacent to the **Select a CSV To Upload** field indicates that the file is 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 managed devices (that were discovered through RSA authentication) in Junos Space, if a new key is generated on Junos Space.

Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space

To upload authentication keys to one or several managed devices manually:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select the devices to which you want to upload authentication keys and click the Upload Keys to Devices icon on the Actions bar.

The Upload Keys to Devices pop-up window is displayed. The IP address of the devices are prepopulated.

3. In the **Device Admin** field, enter the appropriate username for that device.
4. In the **Password** field, enter the password for that device.
5. Confirm the password by reentering it in the **Re-enter Password** field.

6. Select **Next** to provide details for the next device.
7. Select **Upload** to upload the authentication keys to the managed devices.
The Upload Authentication Key dialog box displays a list of 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 the “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.

**Related
Documentation**

- [Key-Based Authentication Overview on page 91](#)
- [Device Discovery Overview on page 109](#)
- [Discovering Devices on page 111](#)
- [Resolving Key Conflicts on page 95](#)

Resolving Key Conflicts

Devices connect to Junos Space Network Management Platform using the RSA Key. When the device is disconnected or down, if 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. On the Junos Space Network Management Platform user interface, 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 Actions menu.
4. Enter the device credentials.

The device is pushed to the Key Based state.

**Related
Documentation**

- [Key-Based Authentication Overview on page 91](#)
- [Changing Device Authentication from Password-based to Key-based Authentication on page 96](#)

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. On the Junos Space Network Management Platform user interface, 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 Actions 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 91](#)

CHAPTER 7

Device Monitoring

- [Viewing and Managing Alarms on page 97](#)

Viewing and Managing Alarms

By default, the Junos Space Network Management Platform is monitored using a built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Monitoring > Node List), and is referred to as the Junos Space Network Management Platform node.

There are two 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, or unacknowledged an alarm, the detailed alarm view displays *admin* instead of the actual remote user in the Acknowledged By field.

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 98](#)
- [Using Alarm Filters to View Alarms on page 99](#)
- [Acknowledging Alarms on page 100](#)
- [Clearing Alarms on page 100](#)

- [Escalating Alarms on page 100](#)
- [Unacknowledging Alarms on page 100](#)
- [Viewing Acknowledged Alarms on page 101](#)

Viewing Alarms

To view alarms:

1. Select **Network Monitoring > Alarms**.
2. Select from any of the following links:
 - All alarms (summary)
 - All alarms (detail)
 - Advanced Search
 - NCS Alarm List

The Alarms page displays 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 16 on page 99](#) 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 16: 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 ID section of the Alarms page.
Severity	Color-coding only	X	Toggle to show only alarms with this severity, or not to show alarms with this severity.
UEI		X	Toggle to show only events with this UEI, or not to show events with this UEI.
Node	X	X	Toggle 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. Toggle 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.

Using Alarm Filters to View Alarms

If you previously created alarm filters, you can select a filter from Alarm Filter Favorites to display the alarms that match the filtering criteria specified in the alarm filter.

To select an alarm filter to view alarms:

1. Navigate to **Network Monitoring > Alarms** and select a filter from Alarm Filter Favorites.
The alarms that match the filtering criteria specified in the alarm filter are displayed.
2. To clear the filter and reset all alarm filtering criteria, select **Remove Filter**.
All outstanding alarms are displayed (the default view).

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 421](#)
- [Managing Alarm Filters](#)

CHAPTER 8

Custom Attributes

- [Adding Custom Labels on page 103](#)
- [Deleting Custom Labels on page 106](#)
- [Modifying Custom Labels on page 107](#)

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 predefined 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 103](#)
- [Adding Custom Labels for Physical Inventory on page 104](#)
- [Adding Custom Labels for a Physical Interface on page 105](#)
- [Adding Custom Labels for a Logical Interface on page 105](#)

Adding Custom Labels for a Device

To add custom labels for a device:

1. On the Junos Space Network Management Platform user interface, select **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 predefined label or add a new custom label.

4. To choose a predefined label:
 - a. Select the predefined label from the **Label Name** drop-down list.
 - b. In the **Value** field, enter an appropriate value.
5. To add a new custom label:
 - a. In the **Label Name** drop-down list, 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. On the Junos Space Network Management Platform user interface, select **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 predefined label or add a new custom label.

5. To choose a predefined label:
 - a. Select the predefined label from the Label Name drop-down list.
 - b. In the **Value** field, enter an appropriate value.
6. To add a new custom label:
 - a. In the **Label Name** drop-down list, 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. On the Junos Space Network Management Platform user interface, select **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 predefined label or add a new custom label.

5. To choose a predefined label:
 - a. Select the predefined label from the Label Name drop-down list.
 - b. In the **Value** field, enter an appropriate value.
6. To add a new custom label:
 - a. In the **Label Name** drop-down list, 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. On the Junos Space Network Management Platform user interface, select **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** drop-down list, 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 11](#)

Deleting 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.

To delete a custom label:

1. On the Network Management Platform user interface, 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 103](#)

Modifying 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.

To modify a custom label:

1. On the Network Management Platform user interface, 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**.

Related Documentation

- [Adding Custom Labels on page 103](#)

CHAPTER 9

Discover Devices

- [Device Discovery Overview on page 109](#)
- [Discovering Devices on page 111](#)

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.

Junos Space can manage devices in either of the following ways:

- Junos Space initiates and maintains a connection to the device.
- The device initiates and maintains a connection to Junos Space.

By default, Junos Space manages devices by initiating and maintaining a connection to the device. When Junos Space initiates the connection to the device, you can discover

and manage devices irrespective of whether the management system is behind a Network Address Translation (NAT) device. For WW Junos devices, Junos Space uses SSH with an adapter to manage the devices.

If device-initiated connection to Junos Space is enabled, the DMI channel and port 7804 are used and the following (sample) configuration is added on the device to establish the connection to Junos Space:

```
set system services outbound-ssh client 0011DOCEFAC device-id 7CE5FE
set system services outbound-ssh client 0011DOCEFAC secret "$ABC123"
set system services outbound-ssh client 0011DOCEFAC services netconf
set system services outbound-ssh client 0011DOCEFAC 172.22.199.10 port 7804
```

To discover and manage devices through a device-initiated connection, clear the **Junos Space initiated connection to device** checkbox on the Modify Application Settings page in the Administration workspace. For information about configuring Space-initiated or device-initiated connections, see [“Modifying Network Management Platform Settings” on page 711](#).



NOTE: Device-initiated connections to a Junos Space system behind a NAT device is not supported.

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 111](#)
- [Viewing Managed Devices on page 14](#)
- [Systems of Record in Junos Space Overview on page 825](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Device Management Overview on page 11](#)
- [Device Inventory Overview on page 12](#)
- [Managing DMI Schemas Overview on page 804](#)

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, credentials to connect to each device (reuse existing credentials or specify new ones), and, optionally probe method (ping or SNMP or both, or none).



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 112](#)
2. [Specifying Probes on page 113](#)
3. [Specifying Credentials on page 114](#)

Specifying Device Targets

To specify the device targets that you want Junos Space Network Management Platform to discover:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Discover Targets**.

The Discover Targets pop-up window is displayed.

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 specify the probes:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Specify Probes**.

The Specify Credentials pop-up window is displayed.

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 pop-up window is displayed.

4. Select the appropriate radio button for the SNMP version.
5. If you select SNMP V1/V2C, specify a community string, which can be **public**, **private**, or a predefined string.
6. If you select SNMP v3:

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.
7. 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 pop-up window is displayed with the configured SNMP settings.

8. 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. To specify the credentials:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Specify Credentials**.

The Specify Credentials pop-up window is displayed.

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.



NOTE: You can check whether a device was discovered and added to Junos Space Network Management Platform, from the Job Details page. To go to the Job Details page, double-click the ID of the device discovery job on the Job Management page. The Description column on this page specifies whether the device was discovered and added to Junos Space Network Management Platform. If the device was not discovered and added to Junos Space Network Management Platform, the column lists the reason for failure. You can also sort all the columns in ascending or descending order to identify the devices that are discovered and devices that are not discovered. To export the device discovery details from the Job Details page, see *Exporting the Device Discovery Details using a CSV File*.

Related Documentation

- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)
- [Device Discovery Overview on page 109](#)

- *Exporting the Device Discovery Details using a CSV File*
- [Viewing Managed Devices on page 14](#)
- [Viewing Scheduled Jobs on page 500](#)
- [Resynchronizing Managed Devices with the Network on page 68](#)
- [Viewing Physical Inventory on page 41](#)
- [Viewing Physical Interfaces on page 44](#)
- [Exporting License Inventory on page 47](#)
- [Managing DMI Schemas Overview on page 804](#)
- [Key-Based Authentication Overview on page 91](#)

CHAPTER 10

Model Devices

- [Model Devices Overview on page 117](#)
- [Creating Connection Profiles on page 118](#)
- [Creating a Modeled Instance on page 122](#)
- [Modifying Connection Profiles on page 124](#)
- [Deleting Connection Profiles on page 124](#)
- [Viewing the Status of Modeled Devices on page 125](#)
- [Adding More Devices to an Existing Modeled Instance on page 126](#)
- [Viewing and Copying Configlet Data on page 127](#)
- [Downloading a Configlet on page 127](#)
- [Activating Devices by Using Configlets on page 129](#)
- [Deleting Modeled Instances on page 131](#)
- [Cloning a Connection Profile on page 132](#)

Model Devices Overview

With the Model Devices feature, you can add multiple devices, specify connectivity parameters, upgrade schema-based configuration on the devices, and upgrade or downgrade the Junos OS version on the devices through a single workflow. This workflow creates a modeled instance and adds the devices to Junos Space Network Management Platform. Devices added using this workflow are known as modeled devices. With this feature, this task is usually accomplished using three different workflows: Device Discovery, Deploy Device Template, and Deploy Device Image.

Currently with the Model Devices feature, you can add ACX Series, EX Series, and SRX Series devices to Junos Space Network Management Platform.

Using the Model Devices feature, you first create a connection profile to specify the connectivity parameters of the device. A connection profile specifies the details of the device interface on which the IP address is configured, the NAT configuration details for Junos Space, and details of the protocol used to assign IP addresses to the devices. You then create a modeled instance that uses the connectivity parameters specified in the connection profile to connect to the devices.

A modeled instance defines the device family for which the configlets are applicable, the Junos OS version that the device will be upgraded or downgraded to, if needed, and the device template containing the common configuration that you want to push to the devices when they are discovered in Junos Space Network Management Platform. You can also specify hostnames, platforms, and authentication details of devices in the modeled instance.

Junos Space Network Management Platform provides you with two options to discover multiple devices with a single modeled instance: using a CSV file or using an in-line editor in the Create Modeled Instance workflow. You can then verify the status of the devices added using the modeled instance with the View Modeled Device Instance task in the Devices workspace. For more information, see [“Viewing the Status of Modeled Devices” on page 125](#). The modeled instance also specifies whether you can choose to validate the serial number and the hostname of the device provided when adding the device with the actual serial name and host name of the device. This way multiple devices are discovered to Junos Space Network Management Platform with the minimum required configuration. This eliminates the need to deploy device templates and upgrade or downgrade device images after the devices are discovered in Junos Space Network Management Platform.

You can download the configlets generated from the modeled instance, modify it on a text editor, and copy it to the CLI console of the device. You can download the configlets in CLI, XML, or curly braces format. You can also encrypt the configlets by using AES. Ensure that your device can decrypt the configlet if you download encrypted configlets.

**Related
Documentation**

- [Creating Connection Profiles on page 118](#)
- [Creating a Modeled Instance on page 122](#)

Creating Connection Profiles

You use a connection profile to specify connectivity-related parameters for devices added to Junos Space Network Management Platform using the Modeling devices feature. A connection profile contains device interface details, the NAT configuration details for Junos Space, and the protocol used to assign IP addresses to devices. You create connection profiles from the Connection Profiles page in the Devices workspace.

To create a connection profile:

1. On the Network Management Platform user interface, select **Devices > Model Devices > Connection Profiles**.

The Connection Profiles page is displayed.

2. Click the Create Connection Profile icon on the Actions menu.

The Create Connection Profile page is displayed.

3. In the **Name** field, enter a name for the new connection profile.

A connection profile name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quotation mark ('), slash (/), and ampersand (&).

4. (Optional) In the **Description** field, enter a description for the new connection profile.
The description cannot exceed 256 characters.
5. Select the type of device interface on which you want to configure the IP address:
Ethernet or **ADSL**.
By default, the Ethernet option button is selected.
6. (Optional) In the **Interface** field, enter the appropriate device interface number..
The default Ethernet interface number is ge-0/0/0. The default ADSL interface number is at-1/0/0.
7. (Optional) If you are using a NAT configuration from Junos Space, select the **NAT'd IP Address for Junos Space** check box to specify the IP address and port number used by the NAT configuration.
8. In the **IP** field, enter the IP address used by the NAT configuration.
9. In the **Port** field, enter the port number used by the NAT configuration.
10. (Optional) From the **IP Assignment via** drop-down list, select how the IP address is assigned to the devices. By default, DHCP is selected. The options presented hereafter depend on the type of device interface on which you configure the IP address and how the IP address is assigned to the devices.

You can assign IP addresses by using the following options for the Ethernet interface:

- Manually (Static)
- Dynamic Host Configuration Protocol (DHCP)
- Point-to-Point Protocol over Ethernet (PPPoE)

You can assign IP addresses by using the following options for the ADSL interface:

- Manually (Static)
- Dynamic Host Configuration Protocol (DHCP)
- Point-to-Point Protocol over ATM (PPPoA)

If you want to assign an IP address to the device manually:

- Select **Static** from the **IP Assignment via** drop-down list

If you select **DHCP** from the drop-down list:

- a. From the **Attempts** selector, use the up and down arrows to specify the maximum number of attempts that the DHCP server will make to reconfigure the DHCP clients before the reconfiguration is considered to have failed.
The default value is 4 attempts.
- b. From the **Interval** selector, use the up and down arrows to specify the initial value in seconds between successive attempts to reconfigure the DHCP clients.
The default value is 4 seconds.

- c. (Optional) Select the **DHCP Server Address** check box to configure the properties of the DHCP server.
- d. In the **IP Address** field, enter the IP address of the DHCP server.
- e. If you want the DHCP clients to propagate the TCP/IP settings to the DHCP server, select the **Update Server** check box.
- f. Select one of the option buttons in the Lease Time section: **Default Value**, **Lease Never Expires**, or **Lease time**. By default, the Default Value option button is selected.

This option specifies the time taken by the DHCP server to negotiate and exchange DHCP messages with the DHCP clients.

- If you want the DHCP server to negotiate and exchange DHCP messages with the DHCP clients, select the **Default Value** option button.
- If you want the DHCP server to assign permanent IP addresses, select the **Lease Never Expires** option button.
- If you want to specify a time interval after which the lease expires, select the Lease Time option button and use the up and down arrows in the **Interval** selector to specify the time interval.

The default value is 4 seconds.

If you select **PPPoE** from the drop-down list:

- a. From the **Authentication Type** drop-down list, select the type of authentication.

Junos Space Network Management Platform supports Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for authentication.
- b. In the **Username** field, enter the username for PPPoE authentication using CHAP.
- c. In the **Password** field, enter the password for PPPoE authentication using CHAP.
- d. In the **Confirm Password** field, reenter the password for PPPoE authentication using CHAP.
- e. In the **Access Profile Username** field, enter the username for PPPoE authentication.

This field is not mandatory for PAP authentication.
- f. In the **Access Profile Password** field, enter the password for PPPoE authentication.

This field is not mandatory for PAP authentication.
- g. In the **Access Profile Confirm Password** field, reenter the password for PPPoE authentication.

This field is not mandatory for PAP authentication.
- h. (Optional) In the **Concentrator Name** field, enter the name of the concentrator.
- i. (Optional) In the **Service Name** field, enter the name of the service you are using.

- j. In the **Auto Connect time Interval** field, use the up and down arrows to specify the time interval in seconds for connecting automatically. The default value is 1 second.
- k. In the **Ideal time before disconnect** field, use the up and down arrows to specify the time interval in seconds before disconnecting. The default value is 1 second.

If you select **PPPoA** from the drop-down list:

- a. From the **Authentication Type** drop-down list, select the type of authentication.
Junos Space Network Management Platform supports Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for authentication.
- b. In the **Username** field, enter the username for PPPoE authentication using CHAP.
- c. In the **Password** field, enter the password for PPPoE authentication using CHAP.
- d. In the **Confirm Password** field, reenter the password for PPPoE authentication using CHAP.
- e. In the **Access Profile Username** field, enter the username for PPPoE authentication.
This field is not mandatory for PAP authentication.
- f. In the **Access Profile Password** field, enter the password for PPPoE authentication.
This field is not mandatory for PAP authentication.
- g. In the **Access Profile Confirm Password** field, reenter the password for PPPoE authentication.
This field is not mandatory for PAP authentication.
- h. In the **VPI** field, use the up and down arrows to specify the Virtual Private Identifier (VPI) for the DSL network of your service provider. The range is 1 to 6000. The default value is 1.
- i. In the **VCI** field, use the up and down arrows to specify the Virtual Channel Identifier (VCI) for the DSL network of your service provider. The range is 1 to 6000. The default value is 1.
- j. From the **Encapsulation Type** drop-down list, select the type of encapsulation: atm-ppp-vc-mux or atm-ppp-llc. atm-ppp-vc-mux provides PPP over ATM AAL5 multiplex encapsulation and atm-ppp-llc provides PPP over AAL5 LLC encapsulation.

11. Click **Create**.

The connection profile is created.

Related Documentation

- [Modifying Connection Profiles on page 124](#)
- [Deleting Connection Profiles on page 124](#)
- [Creating a Modeled Instance on page 122](#)

Creating a Modeled Instance

You create a modeled instance when you want to quickly add multiple devices to Junos Space Network Management Platform using a common set of connectivity parameters. You can add a modeled instance from the Devices workspace.

To create a modeled instance:

1. On the Network Management Platform user interface, select **Devices > Device Management > Model Devices**.

The Model Devices page is displayed.

2. Click the Create Modeled Instance icon on the Actions menu.

The Create Modeled Instance page is displayed.

3. From the **Device Type** drop-down list, select the type of device. The options available are ACX Device, EX Device, and SRX Device.
4. In the **Name** field, enter a name for the modeled instance.

The modeled instance name should start and end with letters or numbers and cannot exceed 255 characters. An underscore (_) is the only special character allowed. Leading and trailing spaces are not allowed.

5. In the **Description** field, enter a description of the modeled instance.
 6. In the **Tag** field, enter a tag for the modeled instance and the modeled devices created in this modeled instance.
 7. Select the **Serial Number Validation** check box if you want to authenticate the device by using the serial number.
- By default, this check box is not selected.

8. Select the **Host Name Validation** check box if you want to authenticate the device by using the hostname.
- By default, this check box is not selected.

9. In the **Username** field, enter the username used to manage to the device.

The maximum length is 255 characters and all characters are allowed. By default, root is the username.

10. Select the **Key Based Authentication** check box if you want to use RSA keys for authentication.

By default, this check box is not selected.

11. In the **Password** field, enter the password used to manage the device.

The maximum length is 20 characters and all characters are allowed.

12. In the **Confirm Password** field, reenter the password used to manage the device.

13. From the **Connection Profile** drop-down list, select a connection profile that specifies the connectivity parameters you want to use for this modeled instance.

If you have not created a connection profile or want to create a new connection profile for this modeled instance, click the **Create** button next to the Connection Profile drop-down list.

The Connection Profile pop-up window is displayed. For more information about creating a connection profile, see [“Creating Connection Profiles” on page 118](#)

14. Select the appropriate option button between **Add Manually** and **Upload CSV** to choose how you want to discover devices to Junos Space Network Management Platform.

- If you want to discover the devices manually, select the **Add Manually** option button.
 - a. In the **Number of Devices** field, use the 'up' and 'down' arrows to specify the number of devices to be discovered using this deployment instance.
 - b. From the **Platform** drop-down list, select the platform for the devices.

- If you want to discover the devices by using a CSV file, select the **Upload CSV** option button.

- a. (Optional) Click the **View Sample CSV** link to download a sample CSV file.

You need to retain the format of the CSV file for the devices to be discovered successfully. You need to enter the name of the devices, serial number of the devices, and the platform of the devices in the CSV file.

- b. Click the **Select a CSV to Upload** link to upload a CSV file.

The Select CSV File pop-up window is displayed.

- c. Click the **Browse** button to browse the file on your computer.

- d. Click **Upload** to upload the CSV file to Junos Space Network Management Platform.

15. (Optional) Select the **Template Association** check box if you want to push some initial configuration to the devices after they are discovered to Junos Space Network Management Platform.

- (Optional) From the **Device Template** drop-down list, select the appropriate device template that contains the configuration that you want to send to the devices.

16. Select the **Image Upgrade/Downgrade** check box if you want to upgrade or downgrade to a common Junos OS version on all devices added using the modeled instance.

- From the **Device Image** drop-down list, select the device image which contains the Junos OS version you want to upgrade or downgrade the devices to.

17. Click **Next**

You can modify the default hostname that is automatically assigned to the device by Junos Space Network Management Platform. You can also modify the platform of the device. If you have selected the Serial Number Validation check box, you need to enter the serial number of the device.

18. Click **Finish**.

The modeled instance is created.

To discover the device to Junos Space Platform, you must download the configlet, copy the configlet to a USB drive, connect the USB drive to the device and reboot the device.

The device connects to Junos Space Platform and is discovered to the Junos Space Platform database during the initial discovery process. For more information about activating devices using configlets, see ["Activating Devices by Using Configlets" on page 129](#).



NOTE: To view the details of the modeled instance, select the modeled instance and select **View Modeled Instance** from the Actions menu.

**Related
Documentation**

- [Model Devices Overview on page 117](#)
- [Adding More Devices to an Existing Modeled Instance on page 126](#)
- [Downloading a Configlet on page 127](#)
- [Viewing and Copying Configlet Data on page 127](#)

Modifying Connection Profiles

You modify a connection profile to change some of the connectivity-related parameters of devices such as device interface details, the NAT configuration details for Junos Space, the protocol used to assign IP addresses to devices. You can modify connection profiles from the Connection Profiles page in the Devices workspace.

To modify a connection profile:

1. On the Network Management Platform user interface, select **Devices > Device Management > Model Devices > Connection Profiles**.

The Connection Profiles page is displayed.

2. Select the connection profile you want to modify and click the Modify Connection Profile icon on the Actions menu.

The Modify Connection Profile page is displayed. You can modify all the fields on this page except the Name field.

3. Click **Modify**.

The connection profile is modified..

**Related
Documentation**

- [Deleting Connection Profiles on page 124](#)
- [Creating Connection Profiles on page 118](#)

Deleting Connection Profiles

You delete a connection profile when you no longer need it to create modeled instances. You can delete connection profiles from the Devices workspace.

To delete connection profiles:

1. On the Network Management Platform user interface, select **Devices > Device Management > Model Devices > Connection Profiles**.

The Connection Profiles page is displayed.

2. Select the connection profile you want to delete and click the Delete Connection Profiles icon on the Actions menu.

The Delete Connection Profiles pop-up window is displayed.

3. Click **Delete**.

The connection profile is deleted.

**Related
Documentation**

- [Modifying Connection Profiles on page 124](#)
- [Creating Connection Profiles on page 118](#)

Viewing the Status of Modeled Devices

You view the status of the devices you added using a modeled instance to view the connection status and managed status of the devices. You can view the status of the devices you added using a modeled instance, from the Devices workspace.

To view the status of the modeled devices added using a modeled instance:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

The Model Devices page is displayed.

2. Select the modeled instance and select **View Modeled Device Status** from the Actions menu.

The View Modeled Device Status page is displayed. This page displays the name of the devices, Junos OS version on the devices, device family, platform of the devices, IP address of the devices, whether the device is connected to Junos Space Network Management Platform, the managed status of the devices, and the serial number of the devices.

3. Click **Back** to return to the Model Devices page.

**Related
Documentation**

- [Model Devices Overview on page 117](#)
- [Creating a Modeled Instance on page 122](#)
- [Adding More Devices to an Existing Modeled Instance on page 126](#)
- [Downloading a Configlet on page 127](#)
- [Viewing and Copying Configlet Data on page 127](#)

Adding More Devices to an Existing Modeled Instance

You add more devices to an existing modeled instance if you want to add devices using the existing parameters of the modeled instance. You can perform this task from the Devices workspace.

To add more devices to a modeled instance:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

The Model Devices page is displayed.

2. Select the modeled instance to which you want to add more devices and select **Add More Devices** from the Actions menu.

The Add More Devices page is displayed. You can view the name of the modeled instance, the device family of the modeled instance, the device template associated with the modeled instance, the device image associated with the modeled instance, and the number of devices that are already part of the modeled instance.

3. (Optional) In the **Apply Tag** field, enter a tag that you want to assign to this modeled instance.
4. In the **Number of Devices to add** field, use the up and down arrows to specify the number of devices that you want to add to this modeled instance.

The default value is zero.

The page is populated with as many rows as the number of devices that you specify in the Number of Devices field. The Hostname, Platform, and OS version columns are populated with default values. You can modify the default hostname, and the platform of the device. If you have selected the Serial Number Validation check box in the modeled instance, you need to enter the serial number of the device.

- If you want to modify the hostname for a device, double-click the hostname of the corresponding device and enter the new hostname
 - If you want to modify the platform for the device, select the appropriate platform for corresponding device from the drop-down list.
 - Click **Update**.
5. Click **Add**.
- The devices are added to the modeled instance.

Related Documentation

- [Model Devices Overview on page 117](#)
- [Creating a Modeled Instance on page 122](#)
- [Downloading a Configlet on page 127](#)
- [Viewing and Copying Configlet Data on page 127](#)

Viewing and Copying Configlet Data

You view the configlet for the modeled instance you created, to copy the configlet data to a text editor for further modifications. From the Devices workspace, you can view the configlet for a modeled instance.

To view and copy configlet data:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

The Model Devices page is displayed.

2. Select the modeled instance whose configlet data you want to view and copy, and select **View Configlet** from the Actions menu.

The View Configlet page is displayed. You can view the name of the modeled instance, number of devices that are part of this modeled instance, and configlet data.

3. From the **Configlet Format** drop-down list, select a format in which you want to view the configlet data.

The options available are CLI, XML, and CURLY BRACES. By default CLI is selected.

4. Copy the configlet data from the Configlet Content field to a Notepad or any other text editor.

If you select to update the configuration in the device template manually, the Configlet Content area displays the configlet containing the connection parameters and the configuration in the device template.

You can modify this configlet as needed and copy the modified data in the configlet to a device's CLI console. The device then connects to Junos Space Platform.

5. Click **Close**.

You are redirected to the Model Devices page.

Related Documentation

- [Model Devices Overview on page 117](#)
- [Creating a Modeled Instance on page 122](#)
- [Adding More Devices to an Existing Modeled Instance on page 126](#)
- [Downloading a Configlet on page 127](#)

Downloading a Configlet

You download a configlet to save a copy of the configlet on your local computer and connect devices to Junos Space Platform. You can download a configlet in XML, CLI, and curly braces formats. You download a configlet from the Devices workspace. Ensure that you temporarily disable the pop-blocker on your browser to be able to download the configlet file on your local computer.

This task is disabled if the modeled device is in the In Sync or Modeled state on the Device Management page.

To download a configlet from the Model Devices page:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

The Model Devices page is displayed.

2. Select the modeled instance whose configlet you want to download and select **Download Configlet** from the Actions menu.

The Download Configlet page is displayed.

3. From the **Configlet Type** drop-down list, select the format of the configlet you want to download.

You can download the configlet in CLI, XML, and curly braces formats.

4. Select whether you want to encrypt the configlet file by selecting the appropriate option button in the Encryption area.

Junos Space Network Management Platform supports encrypting configlets in the AES format.

- To use plain-text, select the **Plain Text** option button.
- To use AES encryption, select the **AES** option button and enter the encryption key in the **Encryption Key** field.

The encryption key must be 16 characters long and can contain letters, numbers, spaces, and special characters.

5. Select how you want to save or copy the configlet file by choosing the appropriate option button in the **Save** area.

- If you select the **None** option button, the configlet file is saved on your local computer.
- If you select the **SFTP** option button, specify the user ID, password, SFTP server IP address, and the file path where you want to save the configlet file on the SFTP server.
- If you select the **FTP** option button, specify the user ID, password, FTP server IP address, and the file path where you want to save the configlet file on the FTP server.

6. Click **Download**.

7. Save the **Configlets.zip** file to your local computer if you want to save it locally.



NOTE: To connect and activate a modeled device from Junos Space Platform, download the configlet in any format, connect a USB device containing the configlet to the device, and reboot the device. The device then connects to Junos Space Platform. For more information, see [“Activating Devices by Using Configlets” on page 129](#).

Related Documentation

- [Model Devices Overview on page 117](#)
- [Creating a Modeled Instance on page 122](#)
- [Adding More Devices to an Existing Modeled Instance on page 126](#)
- [Viewing and Copying Configlet Data on page 127](#)

Activating Devices by Using Configlets

You can activate a modeled device by connecting a USB device containing the configlet generated from the appropriate modeled instance created in Junos Space Network Management Platform. The device then connects to Junos Space Platform through a device-initiated connection.

You can generate a single configlet (per device) or a bulk configlet (one configlet to activate multiple devices).

- Junos Space Platform generates a single configlet if you choose a static connection profile or enable hostname validation and are using a DHCP connection profile.
- Junos Space Platform generates a bulk configlet if you select a DHCP connection profile without hostname validation.



NOTE: If you assigned a device template and selected to deploy the configuration in the device template manually, the configlet contains the connection parameters and the configuration in the device template.

By default, the configlet is downloaded as a .ZIP file in XML, CLI, or curly braces format. You must unzip the .ZIP file and copy the configlet to the USB device before using the configlet to activate devices.

The following tasks describe how to activate modeled devices by using single or bulk configlets.

- [Activating a Device by Using a Plain-text Single Configlet on page 129](#)
- [Activating a Device by Using an AES-encrypted Single Configlet on page 130](#)
- [Activating a Device by Using a Plain-text Bulk Configlet on page 130](#)
- [Activating a Device by Using an AES-encrypted Bulk Configlet on page 131](#)

Activating a Device by Using a Plain-text Single Configlet

A plain text single configlet can be used to activate one device without an encryption key.

To activate a device by using a plain-text single configlet:

1. Copy the plain-text configlet to a USB device.
2. Plug the USB device to the USB port on the device.

3. Power on the device or reboot the device if the device was already powered on.

The configuration in the plain-text single configlet is committed on the device. The device then connects to Junos Space Platform.

Activating a Device by Using an AES-encrypted Single Configlet

An AES-encrypted single configlet can be used to activate one device with an the encryption key.

To activate a device by using an AES-encrypted single configlet:

1. Copy the AES-encrypted configlet to a USB device.
2. Create a text file **Key.txt** containing a 16-digit encryption key on the USB device.
3. Plug the USB device to the USB port on the device.
4. Power on the device or reboot the device if the device was already powered on.

If you did not create the **Key.txt** file on the USB device, you are prompted to enter the 16-digit encryption key.

- Enter the 16-digit encryption key.

The configuration in the AES-encrypted single configlet is committed on the device. The device then connects to Junos Space Platform.

Activating a Device by Using a Plain-text Bulk Configlet

A plain-text bulk configlet can be used to activate multiple devices without an encryption key.

To activate devices by using a plain-text bulk configlet:

1. Copy the plain-text bulk configlet to a USB device.
2. Create a text file **Hostname.txt** containing the hostnames of all devices that should be activated by this configlet, on the USB device.
3. Plug the USB device to the USB port on the device.
4. Power on the device or reboot the device if the device was already powered on.

The configuration in the plain-text bulk configlet is committed on the device. The device then connects to Junos Space Platform.



NOTE: Repeat steps 1 through 4 to activate other devices using the same configlet.

Activating a Device by Using an AES-encrypted Bulk Configlet

An AES-encrypted bulk configlet can be used to activate multiple devices with an encryption key.

To activate devices by using an AES-encrypted bulk configlet:

1. Copy the AES-encrypted bulk configlet to a USB device.
2. Create a text file **Key.txt** containing a 16-digit encryption key on the USB device.
3. Create a text file **Hostname.txt** containing the hostnames of all devices that should be activated by this configlet, on the USB device.
4. Plug the USB device to the USB port on the device.
5. Power on the device or reboot the device if the device was already powered on.

If you did not create the **Key.txt** file on the USB device, you are prompted to enter the 16-digit encryption key.

- Enter the 16-digit encryption key.

The configuration in the AES-encrypted bulk configlet is committed on the device. The device then connects to Junos Space Platform.



NOTE: Repeat steps 1 through 4 to activate other devices by using the same configlet.

Related Documentation

- [Creating a Modeled Instance on page 122](#)
- [Viewing and Copying Configlet Data on page 127](#)

Deleting Modeled Instances

You delete modeled instances when you no longer need them to add devices to Junos Space Network Management Platform. You can delete modeled instances from the Devices workspace.

To delete modeled instances:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.
The Model Devices page is displayed.
2. Select the modeled instances you want to delete and select **Delete Modeled Instances** from the Actions menu.
The Delete Modeled Instances pop-up window is displayed.
3. Click **Delete**.
The modeled instances are deleted.

- Related Documentation**
- [Model Devices Overview on page 117](#)
 - [Creating a Modeled Instance on page 122](#)
 - [Adding More Devices to an Existing Modeled Instance on page 126](#)
 - [Viewing and Copying Configlet Data on page 127](#)

Cloning a Connection Profile

You clone a connection profile when you want to quickly create a copy of an existing connection profile and modify its parameters including the name of the connection profile. You can clone a connection profile from the Devices workspace.

To clone a connection profile:

1. On the Network Management Platform user interface, select **Devices > Device Management > Model Devices > Connection Profiles**.

The Connection Profiles page is displayed.

2. Select the connection profile you want to clone and select **Clone Connection Profile** from the Actions menu.

The Clone Connection Profile page is displayed.

3. Modify the parameters of the connection profile. You can modify all the parameters including the name of the connection profile.
4. Click **Clone**.

A new connection profile is created.

- Related Documentation**
- [Modifying Connection Profiles on page 124](#)
 - [Creating Connection Profiles on page 118](#)

CHAPTER 11

Unmanaged Devices

- [Adding Unmanaged Devices on page 133](#)
- [Modifying Unmanaged Device Configuration on page 136](#)

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.

To add a non-Juniper device to Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Devices > Unmanaged Devices**.

The Add Unmanaged Devices page is displayed.

2. You can add non-Juniper devices either manually or using a CSV file. To add the devices manually, select the **Add Manually** option button.

The Device Details section is displayed on the Add Unmanaged Devices page.

3. Select **Host Name** or **IP Address**.

The first field changes to represent your selection. Enter the appropriate name or address value for the device.

4. (Optional) In the **Vendor** field, 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** check-box, if you want to use SNMP to gather device information. If you do so, the SNMP Settings area is displayed.

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 17 on page 134](#). Enter values as appropriate.

Table 17: 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. To add non-Juniper devices using the CSV file, select the **Import from CSV** option button in the Add Unmanaged Devices page.
9. 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 18 on page 134](#).

Table 18: Sample CSV for Importing Unmanaged Devices

Column Heading	Sample Data	Constraints
Host Name or IP Address	Sunnyvale_R1	Name: Limit of 256 characters, no spaces. IP address: Dotted decimal notation.
Vendor	ABC	Alphabetic characters only
Device UserName	abcd	No validation from Junos Space Platform
Device Password	abcd123	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

Table 18: Sample CSV for Importing Unmanaged Devices (*continued*)

Column Heading	Sample Data	Constraints
SNMP Username	abcde	Username for SNMP V3; otherwise N/A
Authentication Type	MD5	MD5, SHA1, or N/A
Authentication Password	abcde123	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	abcde123	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



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.

10. Once you have a complete CSV file, select **Select a CSV file to Upload**.

11. Click **Next**.

The Add Managed Devices page displays the list of unmanaged devices with their details.

12. Click **Finish**.

You are redirected to the Unmanaged Devices page.

- Related Documentation**
- [Device Management Overview on page 11](#)
 - [Viewing Managed Devices on page 14](#)

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. On the Network Management Platform user interface, 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 **Device Configuration > Unmanaged Device Configuration**. The Modify Unmanaged Device Configuration page is displayed.
3. Modify the unmanaged device configuration.
4. Click **Save**.

- Related Documentation**
- [Device Management Overview on page 11](#)
 - [Viewing Managed Devices on page 14](#)

Secure Console

- [Configuring SRX Device Clusters in Junos Space on page 137](#)

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 137](#)
- [Configuring a Standalone Device from a Two-Node Cluster on page 139](#)
- [Configuring a Primary Peer in a Cluster from a Standalone Device on page 140](#)
- [Configuring a Secondary Peer in a Cluster from a Standalone Device on page 142](#)

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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
2. Select the single-node cluster and select **Device Access > SSH to Device** from the Actions menu.

The SSH to Device pop-up window is displayed.

3. Specify the IP address of the single-node cluster device.

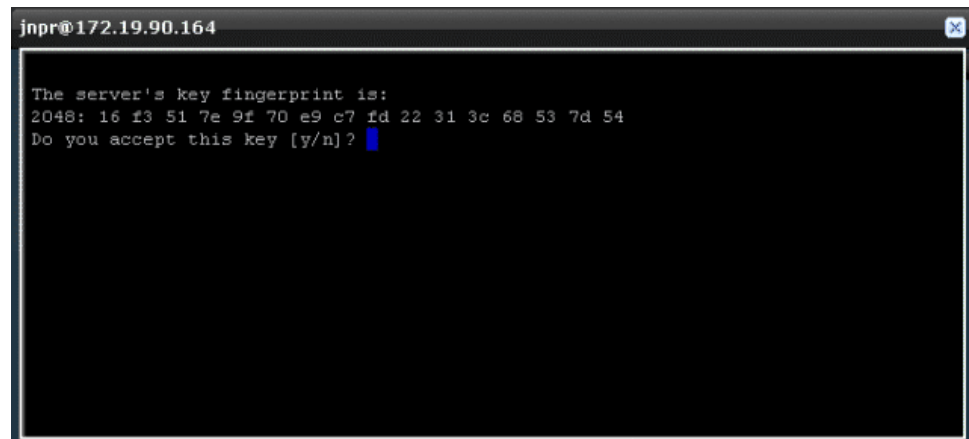


NOTE: A device in a single-node cluster is always the primary member.

4. 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.
5. Click **Connect**.

The device key fingerprint window appears, as shown in the following example.

Figure 3: Validating the Server Key Fingerprint



6. 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.

7. Enter the set chassis command to remove the cluster configuration:
set chassis cluster cluster-id 0 node 0
8. Reboot the device, by entering the command:
request system reboot
9. 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
10. 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
11. 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
12. Delete the outbound-ssh configuration from the group node, for example:
delete groups node0 system services outbound-ssh
13. 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
14. 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

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.

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 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
2. Select the secondary peer device and select **Device Access > SSH to Device** from the Actions menu.

The SSH to Device pop-up window is displayed.

3. Specify the IP address of the secondary peer device.
4. 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.
5. Click **Connect**.

The device key fingerprint window appears, as shown in the following example.

6. 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.

7. Disconnect the HA cable from the device that you want to configure as a standalone device.
8. Enter the set chassis command for the peer device, for example:

set chassis cluster cluster-id 0 node 1

9. Reboot the device, by entering the command:

request system reboot

10. 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 "$ABC123"  
set system services outbound-ssh client 00089BBC494A services netconf  
set system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804
```

11. 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
```

12. 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
```

13. Delete the outbound-ssh configuration from the group level, for example:

```
delete groups node1 system services outbound-ssh
```

14. 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
```

15. 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
```

16. 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.

17. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.

18. 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
2. Select the primary peer in the cluster and select **Device Access > SSH to Device** from the Actions menu.

The SSH to Device pop-up window is displayed.

3. Specify the IP address of the standalone device that you want to configure as the primary peer in the cluster.

4. 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.

5. Click **Connect**.

The device key fingerprint window appears.

6. 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.

7. For the standalone device, enter the command:

```
set chassis cluster cluster-id 1 node 0
```

8. Reboot the device, by entering the command:

```
request system reboot
```

9. 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
```

10. 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
```

11. 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
```

12. Delete the outbound-ssh configuration from the system level, for example:

```
delete system services outbound-ssh
```

13. 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
```

14. Delete the interfaces configuration from the system level, for example:

```
delete interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

15. 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.

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 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. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
2. Select the device and select **Device Access > SSH to Device** from the Actions menu.

The SSH to Device pop-up window is displayed.

3. Specify the IP address of the standalone device that you want to configure as a secondary peer in a cluster.
4. 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.
5. Click **Connect**.

The device key fingerprint window appears.

6. 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.

7. For the standalone device, enter the command:

```
set chassis cluster cluster-id 1 node 1
```

8. Enter the command:

```
request system reboot
```

9. 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
```

10. 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
```

11. 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
```

12. Delete the outbound-ssh configuration from the system level, for example:

```
delete system services outbound-ssh
```

13. 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
```

14. Delete the interfaces configuration from the system level, for example:

```
delete interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

15. Commit the configuration changes on the device again:

```
commit
```

16. Connect the HA cable to each device in the cluster.

17. Establish an SSH connection to the primary device in the cluster.

18. 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.
19. To terminate the SSH sessions, type **exit** from the terminal window prompt, and press Enter.
 20. Click in the top right corner of the terminal window to close the window.

Related Documentation

- [Understanding Logical Systems for SRX Series Services Gateways on page 71](#)

CHAPTER 13

Device Adapter

- [Worldwide Junos OS Adapter Overview on page 145](#)
- [Installing the Worldwide Junos OS Adapter on page 146](#)
- [Connecting to ww Junos OS Devices on page 147](#)

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.

Related Documentation

- [Installing the Worldwide Junos OS Adapter on page 146](#)

Installing the Worldwide Junos OS Adapter

You can install and use the wwadapter to manage devices running on the worldwide version of Junos OS (ww Junos OS devices). Before you install the wwadapter, you must upload the ww Junos OS device wwadapter image file.

To upload the wwadapter image file:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Adapter**.

The Device Adapter page is displayed.

2. Select the Add Device Adapter icon on the Actions 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 Junos Space server.

1. On the server, change the 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 Junos 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 the directories to the wwadapter directory.

```
cd /home/jmp/wwadapter/var/errorLog/DmiAdapter.log
```

To view the contents of the error log file, open the log file with any standard text editor.

To view the contents of the log4j configuration file, change the directories to the wwadapter directory.

```
cd /home/jmp/wwadapter /wwadapterlog4j.lcf
```

Related Documentation

- [Worldwide Junos OS Adapter Overview on page 145](#)

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. On the Junos Space Network Management Platform user interface, select **Administration > Applications**.
The Applications page is displayed.
2. Select **Network Management Platform** and select **Modify Application Settings** from the Actions menu.
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 111), it manages the device just as it would manage a device that runs the domestic version of Junos OS.



NOTE: The SSH to Device option is 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**
- [Worldwide Junos OS Adapter Overview on page 145](#)

CHAPTER 14

Upload Keys to Devices

- [Key-Based Authentication Overview on page 149](#)
- [Generating and Uploading Authentication Keys to Devices on page 149](#)

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 (which uses public-key cryptographic principles). 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 92](#). 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 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.

Junos Space Network Management Platform automates the 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 92](#)

Generating and Uploading Authentication Keys to Devices

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.

- [Generating Authentication Keys on page 150](#)
- [Uploading Authentication Keys to Multiple Managed Devices for the First Time on page 151](#)
- [Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space on page 152](#)

Generating Authentication Keys

To generate a public/private key pair for authentication during login to network devices:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.

The Fabric page is displayed.

2. Click the Generate Key icon on the Actions bar.

The Key Generator pop-up window is displayed.

3. (Optional) In the **Passphrase** field, enter a passphrase to be used to protect the private key, which remains on the system running Junos Space Network Management Platform and is used during device login. 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 impedes an attacker who may gain control of your system and try to log in to your managed network devices.
4. (Optional) Schedule the Junos Space Network Management Platform to generate authentication keys at a later time or immediately.
 - To specify a later start date and time for key generation, select the **Schedule at a later time** check box.
 - To initiate 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 the Junos Space server time but uses the local time zone of the client computer.

5. Click **Generate**.

The Generate Key Job Information dialog box appears, displaying a job ID link for key generation. Click the link to determine whether the key is generated successfully.

Uploading Authentication Keys to Multiple Managed Devices for the First Time

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Click the Upload Keys to Devices icon on the Actions bar.

The Upload Keys to Devices pop-up window is displayed.

3. To upload keys to a single device:

- a. Select **Add Manually**.

The Authentication Details field appears within the Upload Keys to Devices dialog box.

- b. Select **IP Address** or **Hostname**.

- c. In the **IP Address/Host Name** field, enter the IP address or the hostname of the target managed device.

- d. In the **Device Admin** field, enter the appropriate username for that device.

- e. In the **Password** field, 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, CSV file select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

The sample CSV contains the format for entering 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 the “user admin” user on the device.

- c. When 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 a .csv extension.
- e. Click **Upload** to upload the authentication 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 are uploaded and whether this operation is a success.

The green check mark adjacent to the **Select a CSV To Upload** field indicates that the file is 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 managed devices (that were discovered through RSA authentication) in Junos Space, if a new key is generated on Junos Space.

Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space

To upload authentication keys to one or several managed devices manually:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select the devices to which you want to upload authentication keys and click the Upload Keys to Devices icon on the Actions bar.

The Upload Keys to Devices pop-up window is displayed. The IP address of the devices are prepopulated.

3. In the **Device Admin** field, enter the appropriate username for that device.
4. In the **Password** field, enter the password for that device.
5. Confirm the password by reentering it in the **Re-enter Password** field.
6. Select **Next** to provide details for the next device.
7. Select **Upload** to upload the authentication keys to the managed devices.

The Upload Authentication Key dialog box displays a list of 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 the “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.

.....

**Related
Documentation**

- [Key-Based Authentication Overview on page 91](#)
- [Device Discovery Overview on page 109](#)
- [Discovering Devices on page 111](#)
- [Resolving Key Conflicts on page 95](#)

CHAPTER 15

Device Statistics

- [Viewing Device Statistics on page 155](#)

Viewing Device Statistics

You can view the device statistics when you select the Devices workspace. The charts presented on the Devices landing page display the status of the device, and number of devices per OS and number of devices per platform. All the charts are interactive.

The Devices landing page displays the following charts related to 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 the device statistics:

1. On the Junos Space Network Management Platform user interface, select **Devices**.
The Devices landing page is displayed. This page displays the charts related to devices.
2. Click on any of the charts.
You will be redirected to the Devices page.
3. Click the specific label on a chart.
You will be redirected to the Devices page that is filtered based on the label you clicked.

Related Documentation

- [Viewing Managed Devices on page 14](#)
- [Viewing Physical Inventory on page 41](#)
- [Discovering Devices on page 111](#)

CHAPTER 16

QuickView

- [Viewing Devices and Logical Systems with QuickView on page 157](#)

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. On the Network Management Platform user interface, select **Devices > Device Management**.
2. Select the Quick View action button on the menu bar.
3. Alternatively, at the right edge of the Network Management Platform page, 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 71](#)
- [Viewing the Physical Device for a Logical System on page 73](#)
- [Viewing Logical Systems for a Physical Device on page 74](#)
- [Creating a Logical System \(LSYS\) on page 71](#)
- [Deleting Logical Systems on page 72](#)

- *Junos OS Logical Systems Configuration Guide for Security Devices*

CHAPTER 17

Configuration Guides

- [Configuration Guides Overview on page 159](#)
- [Saving the Configuration Created using the Configuration Guides on page 160](#)
- [Deploying the Configuration Created using the Configuration Guides on page 160](#)
- [Previewing the Configuration Created using the Configuration Guides on page 161](#)

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

- [Deploying the Configuration Created using the Configuration Guides on page 160](#)
- [Saving the Configuration Created using the Configuration Guides on page 160](#)

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. On the Junos Space Network Management Platform user interface, select **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 159](#)

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. On the Junos Space Network Management Platform user interface, select **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 159](#)

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. On the Network Management Platform user interface, select **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 159](#)

PART 3

Device Templates

- [Overview on page 165](#)
- [Template Definitions on page 173](#)
- [Device Templates on page 193](#)
- [Quick Templates on page 205](#)

Overview

- [Device Templates Overview on page 165](#)

Device Templates Overview

- [Device Templates Overview on page 165](#)
- [Device Templates Workflow on page 170](#)
- [Viewing Template Definition Statistics on page 171](#)
- [User Privileges in Device Templates on page 172](#)
- [Changing Template Definition States on page 172](#)

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 device template, Device Templates enables you to set all the 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.

Device 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.

You can add and delete configuration details to and from device templates. You can deploy device templates manually, by using tags, or by using a CSV file.

The Templates page in the Device Templates workspace lists the device templates created, in a tabular view. The following [Table 19 on page 165](#) lists the columns in the table along with the description.

Table 19: Templates Page

Column Name	Description
Name	Name of the device template.

Table 19: Templates Page (*continued*)

Column Name	Description
Domain	Domain to which the device template is assigned
Current Version	Current version of the device template
Description	Description of the device template
Device Family	Juniper Networks DMI Schema, for example J/M/MX/T/TX
Last Modified By	Login name of the operator who last modified the device template
Last Update Time	Time when the device template was last updated
Deployment Status	Deployment status of the template
Template Type	Type of device template — Configuration template or Quick template
State	Device template deployment readiness — needs review, disabled, or enabled

Junos Space Network Management Platform assigns different states to the device templates based on the deployment readiness. These states that are indicated in the State column of the table on the Templates page. The following [Table 20 on page 166](#) lists the states and their description.

Table 20: Device Template States

State	Description
Needs Review	The device template cannot be deployed until you review it. This state is triggered by a designer who is modifying the template definition on which the device template is based. That device template is then automatically moved to the Needs Review state.
Disabled	The device template cannot be deployed. This state is triggered by the designer unpublishing the template definition upon which a device template is based. That device template is then automatically disabled.
Enabled	The device template can be deployed. As soon as you finish creating a device template, it is enabled automatically.

The Definitions page in the Device Templates workspace lists the template definitions created, in a tabular view. The following [Table 21 on page 166](#) lists the columns in the table along with the description.

Table 21: Definitions Page

Column Name	Description
Name	Name of the template definition

Table 21: Definitions Page (*continued*)

Column Name	Description
Domain	Domain to which the template definition is assigned
Description	Description of the template definition
Device Family	Juniper Networks DMI Schema, for example J/M/MX/T/TX
Last Modified By	Login name of the template designer who last modified the template definition
Last Update Time	Time when the template definition was last updated
State	State of the template definition — published, or unpublished

Junos Space Network Management Platform assigns different states to the template definitions. These states that are indicated in the State column of the table on the Definitions page. 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.

When you deploy a device template to a device, even the unconfigured parameters are committed. This means that if you applied two device templates to a device, only the configuration contained in the last device template would be retained. For example, if you set SNMP location in the first device template you deployed, but did not do so in the second device template, the SNMP location information would be lost as soon as you deployed the second device template. Therefore, to build up a complex configuration by applying multiple device templates in stages, you should modify the last deployed definition or device template each time you add a layer of complexity.

This behavior also has implications for versioning. For Junos Space Network Management Platform to retain version information, every time a device template is deployed to a device, the previous device template deployed to the device is undeployed, even if the subsequent device template only contains additional parameter settings. In other words, device template deployment is not additive.

The device templates workflow has two [predefined] roles:

- Template Design Manager—A designer who understands both:
 - The technical details of device configuration
 - How to implement this knowledge to solve specific business problems
- 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 device template to configure

one or more devices. The operator then tests the device template on the device (without deploying it). If the device template is validated, the operator deploys the device 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 device 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 device 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, 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: 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 device template if the device template is being edited by another user. You will receive a pop-up message indicating the user who is currently editing the device template.



NOTE: We recommend that you do not navigate to other pages or other Junos Space applications when modifying a device template or a template definition. Save the changes before you navigate to other pages or other Junos Space applications.

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 22 on page 169 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 22: 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.	*	*		*
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.	*	*		*

Table 22: Data Types and Tabs (*continued*)

Data Types	Description	Tabs			
		General	Description	Validation	Advanced
Choice	Choice data type provides a radio button. Check the radio button to use the configuration option in the template.	*	*		*

[Table 23 on page 170](#) lists the validation parameters for the data types supporting validation.

Table 23: 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.

Related Documentation

- [Device Templates Workflow on page 170](#)
- [Creating a Device Template on page 193](#)
- [Creating a Template Definition on page 173](#)

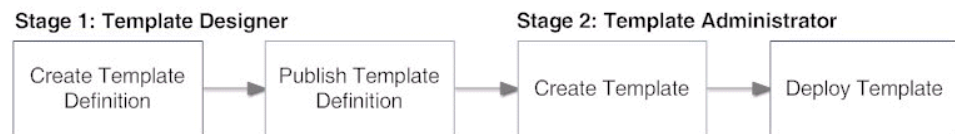
Device Templates Workflow

The device templates workflow has two parts corresponding to the two roles associated with the Device Templates workspace:

- The Template Design Manager, or template designer, who creates the template definition.
- The Template Manager, or template administrator, who creates a template from a template definition.

[Figure 4 on page 171](#) 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 4: Workflow for Device Template Definition and Template Creation



Ensure that the following aspects are considered to use the device template workflows successfully:

- 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

- [Device Templates Overview on page 165](#)
- [Creating a Device Template on page 193](#)
- [Creating a Template Definition on page 173](#)

Viewing Template Definition Statistics

You can view the template definition statistics when you select the Device Templates workspace. The charts presented on the Device Templates landing page display the states of the template definitions. The chart is interactive. Clicking the appropriate label on the Template Definition Status chart, for example, takes you directly to the page displaying that category of template definition. The Template Definition status pie chart shows published and unpublished template definitions (available for template creation and unavailable, respectively).

To view the template definition statistics:

1. On the Junos Space Network Management Platform user interface, select **Device Templates**.

The Device Templates landing page is displayed. This page displays the charts related to device templates and template definitions.

2. Click the Template Definition Status chart.

You will be redirected to the Definitions page.

3. Click the specific label on a chart. For example, click the **Published** label on the Template Definition Status chart.

You will be redirected to the Definitions page that is filtered based on the label you clicked.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Viewing Device Template Statistics on page 203](#)

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 519](#)

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 172](#)

- 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*
 - *Creating a Template*

Template Definitions

- [Creating a Template Definition on page 173](#)
- [Specifying Device-specific Values in Template Definitions on page 179](#)
- [Working with Rules on page 181](#)
- [Finding Configuration Options on page 183](#)
- [Cloning a Template Definition on page 185](#)
- [Deleting a Template Definition on page 186](#)
- [Exporting a Template Definition on page 186](#)
- [Importing a Template Definition on page 187](#)
- [Modifying a Template Definition on page 188](#)
- [Publishing a Template Definition on page 189](#)
- [Managing CSV Files for a Template Definition on page 190](#)
- [Unpublishing a Template Definition on page 191](#)

Creating a Template Definition

You create a template definition to create custom device templates that can be deployed to devices through Junos Space Network Management Platform.

To create a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Click the **Create Template Definition** icon on the Actions bar.

The Create Template Definition page is displayed.

3. From the Device Family Series section, select the device family to which your template definition will apply.

The Junos OS versions and hardware platforms supported by the selected device family appear in the Description section on the right. The OS version that appears on the drop-down list in the OS Version section below the Device Family Series section is the one that is set as default for that device family.



NOTE: It is recommended to include the device family and OS version information in the description of the template definition. Unless you include the information in the definition name or description, the operator will not know which device family this definition applies to.

4. Select the appropriate OS version from the drop-down list in the OS Version section below the Device Family Series section.



NOTE: If you do not use the latest DMI schema, you will not have access to the most recent device configuration options.

5. Click **Next**.
6. In the **Name** field, type a user-defined template definition name.

A template definition name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quote ('), forward slash (/), and ampersand (&).

7. (Optional) In the **Description** field, type a user-defined description. (limit of 255 characters).

The description cannot exceed 256 characters. The operators who use the template definition to create templates rely on the description for information on the template definition.

8. From the Available Configuration section on the left, select one of the following from the drop-down list:

- View All Configuration — provides all configuration options available for the selected device family's default DMI schema.
- Common Configuration — provides 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 — provides 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.

9. Display the hierarchy of Junos OS configuration options available for the device family by clicking the plus sign to the left of Configuration node at the top of the tree.

The hierarchy appears in the form of a tree. Each item can be expanded by clicking the plus sign.

10. (Optional) Click the configuration option that you want to configure for this template definition. To find configuration options, see [“Finding Configuration Options” on page 183](#).

The Selected Configuration Layout section on the right of the page displays the configuration pages. A default page, Config Page 1, is available to hold your groups of configuration options. You can create additional pages by clicking the Add Configuration Page icon at the top of the Selected Configuration Layout section.

11. (Optional) To rename the configuration page and enter a description:
 - a. Select the configuration page in the left panel of the Selected Configuration Layout section.
 - b. In the **Label** field, enter a user-defined configuration page name.
 - c. In the **Description** field, enter a user-defined description.



NOTE: Delete a page by selecting a page from the left panel of the Selected Configuration Layout section and clicking the Delete Selected Page or Option icon.

12. To choose the configurable options, drill down through the hierarchy in the Available Configuration section. Unless you have opened a directory, selecting it and moving it does not transfer the directory's contents into your template definition. You can select multiple options simultaneously by holding down the Ctrl key.

You can move 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.

You can create field labels on the General tab to help the operator enter correct field data. The General tab applies to both the configuration pages and the configuration options you select.

13. To create a field label for configuration options, in the Selected Configuration Layout section, select a configuration option.

The General tab displays the default text.

14. (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 section consider changing the default labels to indicate to operators creating device 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.

15. (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.

16. To save your entries on the General tab, select another tab or another option, or click **Next**.

You can add descriptive text in the Description tab. This can help the operator enter the correct data. When the operator creates a device 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.

17. To change the default description, click the **Description** tab.
18. In the **Description** field, enter a user-defined description for the selected configuration option.
19. To save your the description, move to another tab or another option, or click **Next**.

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. 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. To view the data type correlated to validation criteria, see [“Device Templates Overview” on page 165](#)



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.

20. To modify the details in the Validation tab, click the **Validation** tab.

21. 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.

22. (Optional) For a string, in the **Regular Expression** field, enter a regular expression to further constrain what the operator can enter.

23. (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.

24. To save your entries, select another tab or another option, or click **Next**.

The settings on the Advanced tab determine whether:

- The operator can see the selected option or edit its values.

- Whether 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

25. To modify the details in the Advanced tab, select the **Advanced** tab.

26. Select **Editable**, **Readonly**, or **Hidden**, depending on whether the operator creating the device 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.

27. (Optional) To mark this configuration option as device-specific, click the **Device Specific** check box.

See [“Specifying Device-specific Values in Template Definitions” on page 179](#) 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 181](#) for more information on this.

28. To save your entries, select another tab or another option, or click **Next**.

29. To specify default values for configuration options, select the configuration option.

30. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.

31. (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.

32. 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 22 on page 169](#).

33. 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.

34. 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.

35. (Optional) To verify what the operator sees, click **Operator View**.

36. (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?”

37. (Optional) To save the settings you made in the Operator View, click **Yes**.

38. To complete your definition, return to the designer view by clicking **Designer View**.

39. Click **Finish**

Related Documentation

- [Device Templates Overview on page 165](#)
- [Device Templates Workflow on page 170](#)
- [Creating a Device Template on page 193](#)

Specifying Device-specific Values in Template Definitions

Template designers can use a comma-separated value (CSV) file to provide device-specific values for a template definition. A single CSV file can be used to supply as many values as you wish, because the same file can be used again. Once you have created a CSV file, you import it into Junos Space Network Management Platform, and manage it using the Manage CSV Files task in the Device Templates workspace.

- [Creating a CSV file with device-specific values on page 179](#)
- [Using a CSV file to set device-specific values on page 180](#)

Creating a CSV file with device-specific values

You create a CSV file to import the device-specific values into a template definition. Use one column for each value to be specified and use one row for each device.

To create a CSV file:

1. Open an appropriate program such as Notepad or Microsoft Excel.
2. 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 Junos Space Network Management Platform uses them to identify the values for the template definition.

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**.

3. If you wanted to specify interfaces and other values, you would simply add a column for each type of value, 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 Junos Space Network Management Platform when you choose column and key column.

4. Save the CSV file on your system.

Using a CSV file to set device-specific values

You use the CSV file to set device-specific values in a template definition.

To use a CSV file to set device-specific values in a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Click the **Create Template Definition** icon on the Actions bar.

The Create Template Definition page is displayed.

3. Add the configuration option for which you want to supply device-specific values using a CSV file that you have already created.
4. Click the **Advanced** tab.
5. Select the **Device Specific** check box.
6. Click **Next**.
7. Click the **Device Specific Value** link.

The Device Specific Value - Authorization pop-up window is displayed.

8. Select the **Resolve the value from a CSV file at deploy time** checkbox.

9. Click **Please select a CSV file**.

The Manage CSV files pop-up window is displayed.

Use the Manage CSV files workflow 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.

10. To use a CSV file already in the system, select it and click **OK**.
11. Specify the column and the key column in the CSV file.
12. Select the **Resolve the value from a CSV file at deploy time** check box.

You can now add rules. See [“Working with Rules” on page 181](#) to know how to add, delete, and move rules.

13. Click **Finish**.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Creating a Device Template on page 193](#)

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.

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.

You can add, edit, move, and delete rules. You can only select one rule at a time.

To add a rule:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Click the **Create Template Definition** icon on the Actions bar.

The Create Template Definition page is displayed.

3. Add the configuration option for which you want to supply device-specific values using a CSV file that you have already created.
4. Click the **Advanced** tab.
5. Select the **Device Specific** check box.
6. Click **Next**.
7. Click **Please select a CSV file**.

The Manage CSV files pop-up window is displayed.

Use the Manage CSV files workflow 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.

8. To use a CSV file already in the system, select it and click **OK**.
9. Specify the column and the key column in the CSV file.
10. Select the **Resolve the value from a CSV file at deploy time** check box.

You can now add rules.

11. Click the **[+]** icon.

Two options appear:

- Rule matching tagged device
- Rule matching device name.

12. 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.”

13. Click either **a specific tag** or **a specific value**.

The **Set \$dsv** field appears.

14. 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.

15. 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.

16. (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.

17. (Optional) To delete a rule, select the rule and click the [X] button.

The selected rule disappears.

18. (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.

19. (Optional) Refresh the rules display by clicking the Refresh icon in the lower bar of the Rules section of the Device Specific Value dialog.

20. When you have finished working with rules, close the Device Specific Value dialog box by clicking **Close**.

Related Documentation

- [Device Templates Overview on page 165](#)
- [Device Templates Workflow on page 170](#)
- [Creating a Template Definition on page 173](#)

Finding Configuration Options

You can locate configuration options in two ways: 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 section. 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. You can select a result in three ways:

1. Using the mouse to click on it.
2. Pressing the Enter key to select the first result in the list.
3. 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 screen 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**

- [Device Templates Overview on page 165](#)
- [Device Templates Workflow on page 170](#)
- [Creating a Template Definition on page 173](#)

Cloning a Template Definition

You clone a template definition to quickly create a new template definition with a new name but same properties.

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 188](#)).

To clone a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the template definition you want to clone and select **Clone Template Definition** from the Actions menu.

The Clone Template Definition pop-up window is displayed.

3. (Optional) In the **Please specify a new name for the clone** field, enter a user-defined template definition name.

If you do not enter a new name for the template definition, Junos Space Network Management Platform creates the new template definition by appending “clone of” to the original template definition name.

4. (Optional) In the **Description** field, enter a user-defined description.
5. Click **Clone**.

Related Documentation

- [Device Templates Overview on page 165](#)
- [Creating a Template Definition on page 173](#)

Deleting a Template Definition

You delete a template definition when you no longer need the template definition to propagate the configuration changes to the device template. You can delete a template definition only when it is unpublished.



NOTE: When you delete a template definition, all device templates based on that template definition are permanently disabled. You cannot modify or deploy such templates.

To delete a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the template definition you want to delete and select the Delete Template Definition icon on the Actions bar.

The Delete Template Definitions pop-up window is displayed.

3. Click **Delete**.

Related Documentation

- [Device Templates Overview on page 165](#)
- [Creating a Template Definition on page 173](#)

Exporting a Template Definition

You export a template definition when you want to transfer this template definition to another Junos Space fabric. A template definition retains its state when it is exported.

To export a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the template definition you want to export and select **Export Template Definition** from the Actions menu.

The Export Template Definition pop-up window is displayed.

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 template 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.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Importing a Template Definition on page 187](#)

Importing a Template Definition

You can import template definitions from XML files and export template definitions to XML files. A template definition retains its state when it is exported or imported: published template definitions that are exported also appear as published when they are imported. Therefore, if you import a template 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. You can transfer template definitions from one Junos Space fabric to another.

A template definition is based on a specific OS version, or DMI schema. If the template definition you import is based on a schema that is not found, the template definition is set to the default DMI schema assigned to the device family to which the template definition applies. If you have not set the 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 186](#)).

To import a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the Import Template Definition icon on the Actions bar.

The Import Template Definition page is displayed.

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 template definition, and the name of the template definition.

.....

5. Click **Import**.

**Related
Documentation**

- [Device Templates Overview on page 165](#)
- [Exporting a Template Definition on page 186](#)

Modifying a Template Definition

You modify a template definition when you want to propagate the configuration changes to the device template. You cannot change the device family, OS version, and schema version when modifying the original template definition. When you modify a template definition, you cannot change any existing configuration pages. You can only add new configuration pages.



.....

NOTE: You cannot modify a template definition if the template definition is published. You should first unpublish the template definition before modifying it. If you try to modify a template definition without unpublishing, an error message will be displayed.

.....

To modify a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the template definition you want to modify and click the Modify Template Definition icon on the Actions bar.
3. Modify the parameters you want to modify.
4. Click **Finish**.

After you modify the template definition, republish the associated device templates.

**Related
Documentation**

- [Device Templates Overview on page 165](#)
- [Creating a Template Definition on page 173](#)

Publishing a Template Definition

You publish a template definition when you want to make it available to create device templates from the template definition.

To publish a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the template definition you want to publish and select **Publish Template Definition** from the Actions menu.

The Publish Template Definition page is displayed.

3. Click Publish.

Related Documentation

- [Device Templates Overview on page 165](#)
- [Unpublishing a Template Definition on page 191](#)

Managing CSV Files for a Template Definition

Device Templates uses CSV files to specify device-specific values, in addition to rules (see [“Working with Rules” on page 181](#)). The Managing CSV Files task describes how to import this type of CSV file into Junos Space Network Management Platform. 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 Template Definitions” on page 179](#).

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:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Click the Manage CSV Files icon on the Actions bar.

The Manage CSV File page is displayed.

3. Click **Upload**.

The CSV File upload pop-up window is displayed.

4. Click **Browse**.

The File Upload pop-up window is displayed.

5. Navigate to the desired CSV file, select it and click **Open**.

6. Click **Upload**.

The Manage CSV Files page is displayed. The name of the file just imported appears in the left pane.

7. To display the content of a file, select its name in the left pane.

Related Documentation

- [Device Templates Overview on page 165](#)
- [Device Templates Workflow on page 170](#)
- [Creating a Template Definition on page 173](#)

Unpublishing a Template Definition

You unpublish a template definition when you do not want to make it available to create device templates or when you want to deactivate the device templates that are created based on the template definition.

To unpublish a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

The Definitions page is displayed.

2. Select the template definition you want to unpublish and select **unpublish Template Definition** from the Actions menu.

The Unpublish Template Definition page is displayed. This page also lists the device templates that will be affected if you unpublish the template definition.

3. Click **Unpublish**.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Publishing a Template Definition on page 189](#)

CHAPTER 20

Device Templates

- [Creating a Device Template on page 193](#)
- [Deploying a Template on page 195](#)
- [Undeploying a Device Template on page 197](#)
- [Deleting a Device Template on page 198](#)
- [Modifying a Device Template on page 199](#)
- [Assigning a Device Template to Devices on page 199](#)
- [Unassigning a Device Template From Devices on page 200](#)
- [Viewing Template Deployment Details \(Device Templates\) on page 201](#)
- [Auditing a Device Template Configuration on page 202](#)
- [Viewing Device Template Statistics on page 203](#)

Creating a Device Template

Device templates enable operators to update the Junos OS configuration running on multiple Juniper Networks devices at once. The operators can create and deploy device templates based on template definitions created by designers from the Device Templates workspace.

To create a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Click the Create Template icon on the Actions bar.



TIP: The Create Template page is displayed. This page lists all the template definitions. The operators can only see published template definitions. If you do not see a template definition that you expect to see, the designer might have unpublished it.

3. Select a template definition and click **Next**.
4. In the **Template Name** field, enter a user-defined name for the device template.

The template name is required. The template name must be unique and limited to 63 characters.

5. (Optional) In the **Description** field, enter a user-defined template description.

The template description is optional and limited to 255 characters.

6. Select a configuration page.

The breadcrumb of that page is displayed on the right side of the page. The configuration options are displayed in the pane below the breadcrumbs.



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. You can 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.

7. (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.
8. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.
9. (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.

10. (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.

11. (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).

12. 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.

13. Click **Finish**.

**Related
Documentation**

- [Device Templates Overview on page 165](#)
- [Device Templates Workflow on page 170](#)
- [Creating a Template Definition on page 173](#)

Deploying a Template

Deploying a device template allows the Template Administrator or operator to update the device configuration on multiple devices. Deploying a device template is the second stage of creating a device template. You can deploy a device template when you create it or schedule it to deploy later. Junos Space Network Management Platform allows you to validate the device template against the device.

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.

To deploy a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the device template you want to deploy and select **Deploy Template** from the Actions menu.

The Templates page displays the names of the devices which are compatible to deploy the device template.

3. You can deploy the device template manually, using tags, or by providing a CSV file with filter criteria.

- To deploy the device templates manually, search for compatible devices by entering the search criteria in the search box and clicking the magnifying glass icon.

The list of devices are filtered by the search criteria.

- To filter devices by the device properties, select the check box next to the appropriate device column on the **Column Filter** drop-down list.
- To provide filter criteria using a CSV file, click the CSV Filter icon and upload the CSV file with filter criteria through the Upload a CSV pop-up window.
- To select a device by using tags, select an appropriate tag from the **Tag Filter** drop-down list.

4. Click **Next**.
5. From the left section, select the devices on which you want to deploy the device templates.
6. On the Change Summary tab on the right, click **XML** or **CLI** to see the configuration that will be deployed on the device..
7. Click the **Validate on Device** link to validate the configuration before you deploy it.

By validating the configuration, you ensure that the device template is semantically correct. If the validation results fails, change the template parameters appropriately.
8. Click **Next**.
9. Select whether to deploy the device template now or later or whether to just publish it.
 - To publish the device template, select the **Publish** option button.
 - To deploy the device template now, select the **Deploy Now** option button.
 - To deploy the device template later:
 - a. Select the **Deploy Later** option button.
 - b. Enter the date in the **Date** field in the DD/MM/YYYY format.
 - c. Enter the time in the **Time** field in the hh:mm format.
10. Click **Finish**.

The device template is deployed to the devices.



NOTE: You can check whether a device template is deployed on all devices from the Job Details page. To go to the Job Details page, double-click the ID of the device template deployment job on the Job Management page. The Description column on this page specifies whether the device template id deployed on all the devices. If the device template is not deployed on all devices, the column lists the reason for failure.



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

- [Device Templates Overview on page 165](#)
- [Viewing Template Deployment Details \(Device Templates\) on page 201](#)

- [Undeploying a Device Template on page 197](#)

Undeploying a Device Template

Undeploying a device template allows the Template Administrator or operator to remove the configuration template or quick template from devices on which the device template is deployed.

To undeploy a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the device template you want to undeploy and select **Undeploy Template** from the Actions menu.

The Templates page displays the names of the devices on which the device template is currently deployed.

3. Select the devices from which you want to undeploy the device template.
4. Click **Next**.

The Review Changes page is displayed. You can review the configuration changes that would result from undeploying the template from the selected devices. The following [Table 24 on page 197](#) displays the columns on the Review Changes page.

Table 24: Review Changes Page

Column Name	Description
Device Name	Names of the devices to which the device template was deployed.
Device Specific Value	Name of configuration option to which device-specific values were applied.
Audit Result	Results of the last audit.
Change Summary	summary of changes that will result from undeployment.
Deployed	Configuration pushed to the device when the device template is deployed.
Audit Result	Result of the audit – In sync, Not in sync, or Unavailable.

5. To view the summary of the changes resulting from the undeployment from the device, click on the name of a device in the table on the left of the Review Changes page and select the **Change Summary** tab.
6. To view the device's current configuration, click the **Deployed** tab.
7. To view the audit of the deployment of the current device template to the device, click the **Audit Result** tab.

8. Click **Next**.

The Confirm Undeployment page is displayed.

9. You can select whether to undeploy the device template now or later. If you want to undeploy the device template now, click **Finish**.
10. If you want to undeploy the device template later, select the **Schedule at a Later Time**.
11. Click **Finish**.



NOTE: If a device template is not undeployed from all the devices listed for template undeployment even after using the Undeploy workflow, you can find out the reason by looking at the job details. To view the job details, double-click the job on the Job Management page. The Job Details page is displayed; the Description column specifies the reason why the device template was not undeployed from the devices. The Description column specifies the successful undeployment of device template on a device with the description Template undeployed successfully. You can sort all the columns in ascending or descending order to identify the devices from which the device template was not undeployed.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Deploying a Template on page 195](#)

Deleting a Device Template

Deleting a device template removes the device template from the Junos Space Network Management Platform database. You delete the device template when you no longer want to assign the device template to devices.

To delete a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.
The Templates page is displayed.
2. Select the device template you want to delete and click the Delete Template icon on the Actions bar.
The Delete Templates pop-up window is displayed.
3. Click **Delete**.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Modifying a Device Template on page 199](#)

Modifying a Device Template

You modify a device template to propagate the modifications to the device to which the device template is assigned. If you need to modify the device template after deploying the device template, the Template Designer must check the device template and the template definition to fix any errors. You should redeploy the device template only after the errors are fixed. You can use this workflow to modify both configuration templates and quick templates.

To modify a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the device template you want to modify and click the Modify Template icon on the Actions menu.
3. Modify the device template name, description, or configuration settings.
4. Click **Modify**.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Creating a Device Template on page 193](#)

Assigning a Device Template to Devices

Assigning a device template to a device enables you set up the device template for deployment without actually deploying it or scheduling it for deployment. Assigning a device template places the device 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. A device template that has been assigned to a device cannot be deployed directly. You can use this workflow to assign both configuration templates and quick templates.

To assign a device template to devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the configuration template or quick template to be assigned, and select **Assign to Device** from the Actions menu.

The Template page is displayed. This page displays a table containing only compatible devices, that is, those devices that belong to the same device family as the device template.

3. In the Templates page, select the devices to which the device template is to be assigned.

4. Click **Next**.

The Confirm Assignment page is displayed. This page displays the name of the devices you selected to assign the device template.

5. To confirm the assignment of this device template to this device, click **Finish**.

The Template Assign Confirmation pop-up window is displayed.

6. Click **OK**.

**Related
Documentation**

- [Device Templates Overview on page 165](#)
- [Unassigning a Device Template From Devices on page 200](#)

Unassigning a Device Template From Devices

Unassigning a device template from a device enables you to remove the device template from the device so that it is not considered when deploying the device template to the device. Unassigning a template enables you to remove the template from the queue for the device, so that it can no longer become part of the consolidated configuration changes. You can use this workflow to unassign both configuration templates and quick templates.

To unassign a device template from devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the configuration template or quick template to be unassigned, and select **Unassign to Device** from the Actions menu.

The Template page is displayed. This page displays a table containing only the devices to which the device template is currently assigned.

3. In the Templates page, select the devices from which the device template is to be unassigned.

4. Click **Next**.

The Confirm Unassignment page is displayed. This page displays the name of the devices you selected to assign the device template.

5. To confirm the unassignment of this device template to the selected devices, click **Finish**.

The Template Unassign Confirmation pop-up window is displayed.

6. Click **OK**.

**Related
Documentation**

- [Device Templates Overview on page 165](#)
- [Assigning a Device Template to Devices on page 199](#)

Viewing Template Deployment Details (Device Templates)

Viewing device template deployment enables you to find out which devices a device template has been deployed to, the version of the device template that was deployed to each device, and to find out whether the device was in sync with the device template at the time the last audit was performed, as well as other relevant details.

To get the device template deployment information, you must perform an audit at least once after deploying a device template. To ensure the information presented to you is current, perform a device template configuration audit immediately before viewing the device template deployment information. You can use this workflow to view the deployment details of both configuration templates or quick templates.

To view the device template deployment information:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the configuration template or quick template whose deployment you want to view and select **View Template Deployment** from the Actions menu.

The View Template Deployment page appears. It shows the information described in [Table 25 on page 201](#).

Table 25: View Deployment Table

Column Header	Description
Name	Name of the devices to which the device template is deployed.
IP Address	IP address of the devices to which the device template is deployed.
Template Version	Version of the device template currently deployed to the device named in this row.
Deploy Time	Time at which the device template was deployed to the device named in this row.
Deployed By	Login ID of the person who deployed the device template to the device named in this row.
Job ID	ID of the job constituted by deployment of this device template to the device named in this row.
Audit Status	Audit status of the device template. The states are: <ul style="list-style-type: none"> • Unavailable — Audit is not performed for this device template. • In sync • Not in sync.
Audit Time	Time at which the device template was deployed to the device named in this row.

3. To view details of a device to which the device template was deployed, double-click the device name or its IP address in the View Template Deployment page.

The Device Details pop-up window is displayed.

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

The Template Change Summary pop-up window is displayed. This pop-up window shows the configuration options that were changed when the configuration snippet was deployed to the device.

5. To view the status of the job triggered when the device template was deployed, click the job ID.

The Job Management window appears.

6. To view any differences between a device template and the configuration on the devices to which it is deployed, ensure that an audit has been performed on the device template since it was deployed (see [“Auditing a Device Template Configuration” on page 202](#)).

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

The Template Audit Result pop-up window is displayed.

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

8. To return to the Templates page from the View Template Deployment page, click **Cancel**.

**Related
Documentation**

- [Device Templates Overview on page 165](#)
- [Auditing a Device Template Configuration on page 202](#)

Auditing a Device Template Configuration

You audit a device template configuration to verify the extent to which a device template and the device to which it has been deployed match. The audit can be performed immediately or scheduled for a particular time. Performing an audit immediately before you view device template deployment ensures that you see current information. You can audit a device template configuration only if the device template is deployed. You can use this workflow to audit both configuration templates and quick templates.

To audit a device template configuration:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the configuration template or quick template whose deployment you want to audit and select **Audit Template Config** from the Actions menu.

The Audit Template Configuration pop-up window is displayed.

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**.



NOTE: Device template audit is performed on all the devices associated with the device template. You cannot select individual devices that are associated with the device template for audit.

Related Documentation

- [Device Templates Overview on page 165](#)
- [Creating a Device Template on page 193](#)
- [Deploying a Template on page 195](#)

Viewing Device Template Statistics

You can view the device template statistics when you select the Device Templates workspace. The charts presented on the Device Templates landing page display the states of the device templates and the number of device templates per device family. All the charts are interactive. Clicking the Enabled label on the Template Status chart, for example, takes you directly to the page displaying that category of device template.

The Device Templates landing page displays the following charts related to device templates:

- **Template Status**—this pie chart shows the device templates that are enabled, disabled, and needing review. The device templates based on a template definition that is currently in a published state are enabled. The device templates based on a template definition that is currently unpublished are disabled. The device templates based on a republished template definition are marked as needing review.
- **Template Count by Device Family**—this bar chart shows the number of device templates per device family (each device template can apply to only one device family).

To view the device template statistics:

1. On the Junos Space Network Management Platform user interface, select **Device Templates**.

The Device Templates landing page is displayed. This page displays the charts related to device templates and template definitions.

2. Click the Template Status or Template Count by Device Family chart.

You will be redirected to the Templates page.

3. Click the specific label on a chart. For example, click the **Needs Review** label on the Template Status chart.

You will be redirected to the Templates page that is filtered based on the label you clicked.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Viewing Template Definition Statistics on page 171](#)

CHAPTER 21

Quick Templates

- [Quick Templates Overview on page 205](#)
- [Creating a Quick Template on page 206](#)
- [Deploying a Quick Template on page 210](#)

Quick Templates Overview

With the Quick Template feature, you can use a CLI-based template editor or a form-based editor to send configuration details to multiple devices. You can switch between the two editors to specify the configuration that you want to send. A configuration added from the form-based editor appears in the CLI-based template editor in CLI format and a configuration element added from the CLI-based editor appears as a form in the form-based editor.

You can set default values for variables in the configuration elements and reorder these variables. You use the revised order to display variables when you resolve these variables before deploying them. You can save the variable settings can be saved in a CSV file and download it to the local computer.

You can deploy quick templates on devices by searching devices, selecting devices, by filtering devices by their properties such as device name, connection status, managed status, OS version, IP address, and platform, by tags, or by providing a CSV file with filter criteria. Before you deploy the configuration to the devices, resolve the variables in the configuration elements manually, using tags, or by uploading a CSV file that specifies how to resolve the variables. You can choose to deploy the configuration immediately, or at a later time, or just publish the quick template.

You can create a Quick template based on the current configuration on a managed device by using the Create Template from Device Configuration workflow (**Devices > Device Management > Device Configuration > Create Template from Device Configuration**) from the Devices workspace.

You cannot copy the configuration from the CLI-based template editor directly to the CLI console of a device. To successfully copy and commit the configuration, copy the configuration from the CLI-based template editor to a text file before copying the configuration to the CLI console of a device.

- Related Documentation**
- [Creating a Quick Template on page 206](#)
 - [Deploying a Quick Template on page 210](#)

Creating a Quick Template

Quick templates enable you create a device template without using a template definition. You can create and deploy quick templates from the Device Templates workspace.



NOTE: To create a Quick template based on the current configuration on a managed device by using the Create Template from Device Configuration workflow, click **Devices > Device Management > Device Configuration > Create Template from Device Configuration** from the Devices workspace. You are directed to the Create Quick Template page.

To create a quick template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.
The Templates page is displayed.
2. Click the 'down' arrow next to the Create Template icon on the Actions bar and select **Create Quick Template**.
The Quick Template page is displayed.
3. In the **Name** field, enter a name for the quick template.
The quick template name is required. The quick template name must be unique and limited to 63 characters.
4. (Optional) In the **Description** field, enter a description of the quick template.
The description is optional and limited to 255 characters.
5. From the **Device Family** drop-down list, select an appropriate device family.
6. From the **Versions** drop-down list, select an appropriate Junos OS version.
7. Create a quick template by using the CLI-based template editor or the form-based template editor.

To create a quick template by using the CLI-based template editor:

- a. Click the **CLI-based Template Editor** link.

The CLI-based Template Editor is displayed. The left section of the Template Editor is a text editing area. You can type or paste Junos OS CLI commands in this section. A tool bar at the top of the text area provides functionalities such as save, syntax validation, copy, paste, cut, undo, redo, and find. The right section of the Template Editor provides configuration options such as Access profile, Class of service, and Firewall. The configuration options available here depend on the device family you selected.

- b. Navigate through the configuration option levels and double-click the configuration option you want to add to the quick template.

The selected configuration option is displayed in the CLI-based template editor. You can edit this configuration option.

- c. Use the tool bar functionalities to modify the configuration on the CLI-based template editor.

To create a quick template using the form-based template editor:

- a. Select the **Basic Setup** link.

The Basic Setup pop-up window is displayed.

- b. (Optional) In the **Hostname** field, enter the hostname of the device.
- c. (Optional) In the **Domain name** field, enter the domain name of the device.
- d. (Optional) In the **Timezone** field, enter the hostname of the device.
- e. (Optional) Select the **Allow FTP file transfers** check-box if you want to allow FTP file transfers on the device.
- f. (Optional) Select the **Allow ssh access** check-box if you want to allow accessing the device using SSH.
- g. (Optional) Select the **Allow telnet login** check-box if you want to allow logging into the device using Telnet.
- h. In the NTP Server section, click the Add NTP Server icon to add an NTP server to the device.

The Add pop-up window is displayed. Enter the following details in this pop-up window.

- a. In the **Name** field, enter the name of the NTP server.
- b. (Optional) In the **Key** field, enter a value for the key.
- c. (Optional) From the **Version** drop-down list, select the appropriate version.
- d. (Optional) Select the **Prefer** check-box is required.
- e. Click **Create**.

Use the Edit NTP Server and Delete NTP Server icons to edit and modify the NTP server details respectively.

- i. In the User Management section, click the Add User icon to add users for the device.

The Add pop-up window is displayed. Enter the following details in this pop-up window.

- a. In the **Name** field, enter the name of the user.
- b. (Optional) Select an appropriate user ID from the **User ID** field.

The minimum value for this field is 100.

- c. (Optional) In the **Full Name** field, enter the full name of the user.

- d. (Optional) In the **Password** field, enter the password for the user.
- e. (Optional) In the **Re-enter Password** field, re-enter the password for the user.
- f. From the **Login Class** drop-down list, select the appropriate login class for the user.

The available login classes are super-user, operator, read-only, unauthorized, and wheel.

- g. Click **Create**.

Use the Edit User and Delete User icons to edit and modify the details of the user respectively.

- j. In the DNS Server section, click the DNS NTP Server icon to add a DNS server to the device.

The Add pop-up window is displayed. Enter the following details in this pop-up window.

- a. In the **Name** field, enter the name of the DNS server.
- b. Click **Create**.

Use the Edit DNS Server and Delete DNS Server icons to edit and modify the DNS server details respectively.

- k. Enter the following details In the SNMP section:

- 1. In the **Location** field, enter the location for SNMP..
- 2. Click the Add SNMP Community icon.

The Add pop-up window is displayed. Enter the following details in the Community section:

- a. In the **Name** field, enter the name of the SNMP community.
- b. (Optional) From the **Authorization** drop-down list, select the appropriate type of authorization.
- c. Click **Create**.

Use the Edit SNMP Community and Delete SNMP Community icons to edit and modify the SNMP Community details respectively.

- 3. Click the Add Trap Group icon.

The Add pop-up window is displayed. Enter the following details in the Trap Group section:

- a. In the **Name** field, enter the name of the trap group.
- b. (Optional) Select the check-box next to the appropriate trap group category.
- c. Click **Create**.

Use the Edit Trap Group and Delete Trap Group icons to edit and modify the trap group details respectively.

- l. Click **OK**.



NOTE: If you have installed the Security Director application on your Junos Space Network Management Platform setup and are creating a quick template by choosing J/SRX/LN as the device family, you can use the additional Configuration Guides available on the Create Quick Template page. In this case, the Create Quick Template page lists the Configuration Guides to setup routing and security parameters for the quick template. For more information on using the Configuration Guides related to routing and security parameters for the quick template, see the Junos Space Security Director Application Guide.



NOTE: The Basic Setup configuration guide is only available when ACX/J/M/MX/T/TX/PTX/EX92xx, EX, J/SRX/LN, QF, and QFX is selected as the device family.

8. When you have configured all configuration options required for the quick template, click **OK**.
9. (Optional) Click the **Variable Settings** button on the lower left to configure the order of the variables and the default value for these variables.

The Variable Settings pop-up window is displayed. You can view all the variables you want to use in the configuration in the Variables section on the left and view the Variable Settings section on the right. To configure variable settings:

- a. To reorder variables, use the up and down arrows in the Variables section.
- b. (Optional) In the **Display Name** field, enter a user-defined display name.
- c. (Optional) In the **Default Value** field, enter the default value of the variable.
- d. (Optional) In the **Valid RegEx** field, enter a regular expression.
- e. (Optional) You can either save these variable settings and revisit them later or download to your computer in CSV format.
 - (Optional) To download the variables and their settings in CSV format, click the **Generate CSV Format** button.
 - (Optional) To save the variables and their settings without downloading, click the **Save** button.
10. (Optional) Preview the configuration before saving it by clicking the **Preview** button.
11. You can save the quick template for future modifications, or immediately deploy the quick template to devices.
 - To save the quick template, click **Save**.

- To deploy the quick template, click **Save and Publish/Deploy**.

You are redirected to the Deploy Template page. Deploy the quick template. For more information on how to deploy the configuration template, see [“Deploying a Quick Template” on page 210](#)

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Creating a Device Template on page 193](#)

Deploying a Quick Template

You deploy a quick template after you create it. The deployed quick template enables the Template Administrator or operator to update device configuration details on multiple devices.

To deploy a quick template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

The Templates page is displayed.

2. Select the quick template that you want to deploy and select **Deploy Template** from the Actions menu.

The Templates page displays the names of devices to which you can deploy the quick template.

3. You can deploy the quick template to these devices manually, by using tags, or by providing a CSV file with filter criteria.

- a. To manually deploy quick templates, search for compatible devices by entering the search criteria in the search box and clicking the magnifying glass icon.

The list of devices are filtered by the search criteria.

- b. To filter devices by device properties, select the check box next to the appropriate device column on the **Column Filter** drop-down list.

- c. To select a device by using tags, select an appropriate tag from the **Tag Filter** drop-down list.

- d. To provide filter criteria through CSV file, click the CSV Filter icon and upload the CSV file with the filter criteria by using the Upload a CSV pop-up window.

4. Select the devices on which you want to deploy the device templates and click **Next**.
5. Select the device on the left and Click **XML** or **CLI** to see the configuration that will be deployed on the device.
6. Click the **Validate on Device** link to validate the configuration before you deploy it.

By validating the configuration, you ensure that the device template is semantically correct. If the validation fails, change the template parameters appropriately.

7. Click **Next**.

8. Select whether to deploy the quick template now or later or whether to just publish it.
 - To publish the quick template, select the **Publish to pending configuration changes** option button.
 - To deploy the quick template now, select the **Deploy Now** option button.
 - To deploy the quick template later:
 - a. Select the **Deploy Later** option button.
 - b. Enter the date in the **Date** field in the DD/MM/YYYY format.
 - c. Enter the time in the **Time** field in the hh:mm format.
9. Click **Finish**.

- Related Documentation**
- [Device Templates Overview on page 165](#)
 - [Creating a Quick Template on page 206](#)

PART 4

CLI Configlets

- [CLI Configlets Overview on page 215](#)
- [Managing CLI Configlets on page 225](#)
- [Configuration Views Overview on page 243](#)
- [Managing Configuration Views on page 249](#)
- [XPath and Regex on page 257](#)
- [Configuration Filter on page 261](#)

CHAPTER 22

CLI Configlets Overview

- [CLI Configlets Overview on page 215](#)
- [CLI Configlets Workflow on page 216](#)
- [Configlets User Roles on page 219](#)
- [Configlet Context on page 220](#)
- [Nesting Parameters on page 223](#)

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. A 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	Name of the host on which the CLI configlet is applied
\$INTERFACE	Name of the interface for which the configlet is applied
\$UNIT	Unit number of the logical interface for which the configlet is being applied
\$CONTEXT	Context of the element for which the configlet is applied

User defined Variables

The values for these variables are entered by the user at execution time. Text fields or Selection fields are used to retrieve data 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 as 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/releases/velocity-1.4/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

- *Viewing CLI Configlet Statistics*

CLI Configlets Workflow

A configlet can be defined from the configlet workspace. [Table 26 on page 217](#) lists the parameters to be defined for a configlet.

Table 26: 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 retrieved from the environment or entered by the user during execution. Parameters appear in the second step in the create/edit CLI configlet wizard. While applying configlets, the user is asked to input values for all the variables defined in the configlet.

To configure a parameter, click the modify icon on the toolbar. The Edit Configlet Parameter screen is displayed. 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 is displayed. 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. Local variables have to be deleted manually or set to type “Invisible”.

Table 2 lists the attributes of the configlet parameters.

Table 27: Attributes of 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 provide 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 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, 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) in order to fetch the value from the array. Eg: \$INTERFACE.get(0)</p>
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.

Table 27: Attributes of Configlet Parameters (*continued*)

Configlet Parameter Attributes	Description
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 CLI configlet to the device.

Related Documentation • [Viewing CLI Configlet Statistics](#)

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 **Network Management Platform > Role Based Access Control > Users**. The Manage Users page lists the existing users. Use this page to create and assign roles to the Configlets users.

[Table 28 on page 219](#) describes the Configlets tasks that different users have access to, based on the roles assigned to them.

Table 28: Configlets User Roles Permissions

User Role	Permitted Tasks
CLI Configlets Manager	Viewing, creating, modifying, cloning, deleting, compare versions, Import, Export, applying configlets
CLI Configlets Operator	Applying CLI configlets.

Related Documentation • [Viewing CLI Configlet Statistics](#)

Configlet Context

Execution of scripts and CLI configlets may be required in some case. 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 called device. This includes configuration xml, interface-information xml, chassis-inventory xml and system-information xml.

An example of a device XML is as follows:

```
<device>
<interface-information>.....</interface-information>
<system-information>.....</system-information>
<chassis-inventory>.....</chassis-inventory>
<configuration>.....</configuration>
....
</device>
```

[Table 29 on page 220](#) shows the commands to view the XML from the CLI of the device.

Table 29: Commands to View XML from the 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 the system information XML is as follows:

```
<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

There is a need to have the 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 only to the interfaces that are enabled. Having a context associated with the script or configlet solves this scoping problem.

The 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 Path
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
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) it is 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 considered a match.

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 in devices.

Physical Interface 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 node below. 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>

```

Physical Interface in “up” state:

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 it.

- Related Documentation**
- [CLI Configlets Overview on page 215](#)
 - [CLI Configlets Workflow on page 216](#)

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.

A configlet could refer another configlet present in Junos Space Network Management Platform using the following statement.

```
#include_configlet("<CONFIGLET-NAME>")
```

Junos Space Network Management Platform would merge the referred configlets inline.

Create a configlet named 'SayHello'

```
#set( $person = "Bob" )  
Hello $person
```

Create another configlet named 'Greeting'

```
This is a greeting example  
#include_configlet("SayHello")
```

When the configlet 'Greeting' gets evaluated, it generates the following string.

```
This is a greeting example  
Hello Bob
```

Related Documentation

- [CLI Configlets Overview on page 215](#)

CHAPTER 23

Managing CLI Configlets

- [Creating a CLI Configlet on page 225](#)
- [Applying a CLI Configlet to a Device on page 228](#)
- [Cloning a CLI Configlet on page 229](#)
- [Deleting CLI configlets on page 230](#)
- [Importing a CLI Configlet on page 230](#)
- [Modifying CLI Configlets on page 231](#)
- [Exporting CLI Configlets on page 232](#)
- [Comparing CLI Configlet Versions on page 232](#)
- [Viewing CLI Configlet Statistics on page 234](#)
- [CLI Configlet Examples on page 234](#)

Creating a CLI Configlet

You create a CLI configlet from the Configlets workspace. Parameters are the variables defined in the configlet whose values are either got from the environment or given by the user during execution.

To create a CLI configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets** > **Configlets**.

The Configlets page is displayed.

2. Click the Create CLI Configlet icon from the Actions menu.

The Create CLI Configlet page is displayed.

3. In the **Name** field, enter a name for the CLI 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.

4. In the **Category** field, enter a name for the category you want to associate this CLI configlet to.

The Category of the configlet. The Category cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).

5. From the **Device Family Series** drop-down list, select the device family for which you want to create the CLI configlet.
6. (Optional) From the **Context** drop-down list, select the appropriate context for this CLI configlet.
7. (Optional) In the **Description** field, enter a description.

The description cannot exceed 2500 characters.

8. Select the appropriate type of execution from the Execution Type section. The option buttons available are **Single** and **Grouped**.
9. For Preview options, select the check boxes if you want to view the parameters and the configuration in the CLI Configlet before applying the configuration to devices.

The check boxes available are **Show Parameters** and **Show Configuration**.

10. For Postview options, select the check boxes if you want to view the parameters and the configuration in the CLI Configlet in the Apply CLI Configlet job results.

The check boxes available are **Show Parameters** and **Show Configuration**.

11. Click **Next**.

The Add Configlet Parameter pop-up window is displayed.

12. Configure the parameter you want to use in the CLI configlet.

- a. Click the Add Parameter icon to add a new parameter.
- b. In the **Parameter** field, enter the name of the parameter.
- c. In the **Display Name** field, enter a display name for this parameter.
- d. In the **Description** field, enter a description for this parameter.
- e. From the **Parameter Scope** drop-down list, select an appropriate scope for the parameter.
- f. From the **Parameter Type** drop-down list, select an appropriate type of parameter.
 - **Text Field** – you can provide your own value.
 - **Selection Field** – you can select a value from a set of options.
 - **Invisible Field** – refers to a value either defined explicitly or by an XPath.
- g. From the **Regex Value** drop-down list, select an appropriate regular expression value.
- h. From the **Configured Value XPath** drop-down list, select an appropriate xpath value.

This field is enabled only when you choose the type of parameter as a Selection field. This field contains the XPath (with reference to device xml) to fetch the set of values for the Selection field.

- i. In the **Default Value** field, enter a 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.

- j. From the **Selection Values XPath** drop-down list, select an appropriate xpath value.

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.

- k. In the **Selection Values** field, enter an appropriate selection value.

- l. In the **Order** field, enter the order in which the parameters would be listed while applying.

- m. Click **Add**.

13. (Optional) Add multiple parameters.

14. Click **Create**.

The CLI configlet is created.



NOTE: To view the details of the CLI configlet, select the CLI configlet and select the View CLI Configlet icon from the Actions menu.



NOTE: To assign the CLI configlet to a domain, select the CLI configlet and select the Assign CLI Configlet to domain from the Actions menu.

Related Documentation

- [CLI Configlets Overview on page 215](#)
- [Applying a CLI Configlet to a Device on page 228](#)
- [Exporting CLI Configlets on page 232](#)

Applying a CLI Configlet to a Device

You apply a CLI configlet to a device when you want to push the configuration in the CLI configlet to the device. You can also apply a CLI configlet to multiple devices. The type of execution specified in the CLI configlet determines whether the CLI configlet can be applied to multiple devices or a single device. If the type of execution is Single, the CLI configlet can be applied to a single device. If the type of execution is Grouped, the CLI configlet can be applied to multiple devices.

To apply a CLI configlet to a device:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Select the CLI configlet you want to apply to a device.

The Apply CLI Configlet page is displayed.

3. Select the devices on which you want to apply the CLI configlet and select **Apply CLI Configlet** from the Actions menu.

You can also select multiple device if you want to push the configuration to multiple devices.

The Apply CLI Configlet page displays the parameters. Only text field and selection field type parameters are displayed

To view the description of the parameter, hover the mouse over the entry in the Parameter column.

4. Double-click the **Value** column for each parameter and enter a value.

All values are accepted for the text field type parameter. For a selection field type parameter, you should select from one of the values you provided for the parameter. The set of values present and the default value selected is defined when creating a template.

5. Click **Next**.

The parameter value is validated against the regular expression (if given). If the parameter value violates the regular expression then validation error is displayed.

The Preview section of the Apply CLI Configlet page displays the preview of the CLI configlet. If you selected to view the parameters and the configuration when previewing the CLI configlet, the parameters and the configuration are displayed.



NOTE: Contents of the Preview section depend on the preview options in the CLI configlet.

6. (Optional) Click **Validate** to validate the configuration.

The Validate Configlet progress bar is displayed. When the validation is complete, the Validation Result pop-up window is displayed. This window displays the validation results.

7. Select whether to apply the CLI configlet now or later.

- To apply the CLI configlet now:

- Click **Apply**.

The Configlets Results page is displayed. This page shows the job results.

- Click **Close** to return to the Configlets page.

- To apply the CLI configlet later:

- a. Click **Back**.
- b. Select **Schedule at a later time**.
- c. Enter the date in the **Date** field in the DD/MM/YYYY format.
- d. Enter the time in the **Time** field in the hh:mm format.
- e. Click **Apply**.

The Job Information pop-up window is displayed.

- f. Click **OK**.

Related Documentation

- [CLI Configlets Overview on page 215](#)
- [Creating a CLI Configlet on page 225](#)
- [Exporting CLI Configlets on page 232](#)

Cloning a CLI Configlet

You clone a CLI configlet when you want to create a copy of an existing CLI configlet.

To clone a CLI configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Select the CLI configlet you want to clone and select **Clone CLI Configlet** from the Actions menu.

The Clone CLI Configlet page is displayed. You can modify all the fields of the CLI configlet.

3. Modify the **Name** field.
4. (Optional) Modify the other fields in the CLI configlet and click **Next**.

5. (Optional) Add, modify, or delete the necessary fields.
6. Click **Create**.

The new CLI configlet is created.

- Related Documentation**
- [CLI Configlets Overview on page 215](#)
 - [Creating a CLI Configlet on page 225](#)
 - [Exporting CLI Configlets on page 232](#)

Deleting CLI configlets

You delete CLI configlets when you no longer want to use them to apply configuration to devices.

To delete CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Select the CLI configlets you want to delete and select the Delete CLI Configlets icon from the Actions menu.

The Delete CLI Configlet pop-up window is displayed.

3. Click **Confirm**.

The CLI configlets are deleted.

- Related Documentation**
- [CLI Configlets Overview on page 215](#)
 - [Creating a CLI Configlet on page 225](#)
 - [Exporting CLI Configlets on page 232](#)

Importing a CLI Configlet

You import a CLI configlet XML file to add a CLI configlet to the Junos Space Network Management Platform database. You can also import multiple configlets in a single XML file.

To import a CLI configlet to Junos Space Network Management Platform:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Select the Import CLI Configlet icon from the Actions menu.

The Import CLI Configlet page is displayed.

3. To select the CLI configlet XML from the local computer, click **Browse** and select the CLI configlet XML.



NOTE: Click the View Sample XML link to view and download the sample XML file. You can modify the sample XML file to create new CLI configlet XMLs.

4. Click **Import**.

The Import CLI Configlet progress bar is displayed.



NOTE: Junos Space Network Management Platform validates the fields in the CLI configlet XML file for acceptable values and checks if an identical CLI configlet XML already exists. A Validation error is displayed if any field contains incorrect values. If an identical CLI configlet XML already exists, the Configlet Already Exists pop-up window is displayed. To overwrite the existing XML file, click OK. To cancel the import, click Cancel.

If all fields in the XML file are validated and an identical XML file does not exist, the XML file is imported to Junos Space Network Management Platform.

5. Click **OK**.

Related Documentation

- [CLI Configlets Overview on page 215](#)
- [Applying a CLI Configlet to a Device on page 228](#)
- [Exporting CLI Configlets on page 232](#)

Modifying CLI Configlets

You modify a CLI configlet when you want to change the properties of the CLI configlet.

To modify a CLI configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Select the CLI configlet you want to modify and select the Modify CLI configlet icon on the Actions menu.

The Modify CLI configlet page is displayed.

3. Modify the CLI configlet properties and click **Update**.

The CLI configlet is modified.

Related Documentation

- [CLI Configlets Overview on page 215](#)

- [Creating a CLI Configlet on page 225](#)
- [Exporting CLI Configlets on page 232](#)
- [Importing a CLI Configlet on page 230](#)

Exporting CLI Configlets

You export the CLI configlets when you want to download a copy of the CLI configlets to your local computer.

To export CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. You can select and export specific CLI configlets or export all configlets on the Configlets page.

- To export specific CLI configlets:

- a. Select the CLI configlets and select **Export Selected CLI Configlets** from the Actions menu.

The Export CLI Configlets pop-up window is displayed.

- b. Click **Export** and save the file on your local computer.

- To export all CLI configlets:

- a. Select **Export All CLI Configlets** from the Actions menu

The Export CLI Configlets pop-up window is displayed.

- b. Click **Export** and save the file on your local computer.

The CLI configlets are exported.

Related Documentation

- [CLI Configlets Overview on page 215](#)
- [Creating a CLI Configlet on page 225](#)

Comparing CLI Configlet Versions

You compare CLI configlets when you want to view the difference in the configuration it contains. You can compare two different CLI configlets or compare two version of the same CLI configlet.

To compare CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets** > **Configlets**.

The CLI Configlets page is displayed.

2. Select the CLI configlet that you want to compare and select **Compare CLI Configlet Versions** from the Actions menu.

The **Compare CLI Configlet Versions** page is displayed.

3. Use the **Source CLI Configlet** and **Target CLI Configlet** lists to select the CLI configlets that you want to compare.
4. Use the **Version** lists to specify the versions of the source and target CLI configlets that you have selected.
5. Click **Compare..**

The Compare CLI Configlets window is displayed. This window displays differences between the CLI configlets.

The differences between the two CLI configlets are represented using three different colors:

- Green—The green lines represent the changes that appear only in the source CLI configlet.
- Blue—The blue lines represent the changes that appear only in the target CLI configlet.
- Purple— The purple lines represent the changes that are different between the two CLI configlets.

After the **Next Diff** and **Prev Diff** buttons, the total number of differences, the number of differences in the source CLI configlet, the number of differences in the target CLI configlet, and the number of changes are displayed.

6. Use the **Next Diff** and **Prev Diff** buttons to navigate to the next change or the previous change, respectively.
7. Click **Close** to close the window and return to the Compare CLI Configlet Versions page.

**Related
Documentation**

- [CLI Configlets Overview on page 215](#)
- [Creating a CLI Configlet on page 225](#)
- [Exporting CLI Configlets on page 232](#)

Viewing CLI Configlet Statistics

You can view the statistics about the CLI configlets from the CLI Configlets workspace. The CLI Configlets landing page displays the CLI Configlet Count by Device Family bar chart. The bar chart shows the number of CLI Configlets on the y axis and device family series on the x axis.

To view the statistics of CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets**.

The CLI Configlets landing page is displayed. This page displays the charts related to CLI configlets and configuration views.

2. Click the CLI Configlet Count by Device Family chart.

You will be redirected to the Configlets page.

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.

Related Documentation

- [CLI Configlets Overview on page 215](#)
- [Creating a CLI Configlet on page 225](#)
- [Exporting CLI Configlets on page 232](#)

CLI Configlet Examples

- [CLI Configlet Examples on page 234](#)

CLI Configlet Examples

Default Configlets are added during server start up or data migration. These default configlets are added only on the initial server start up and during data migration. The user can perform all the usual operations on the default Xpath and Regex, including delete operation.

Adding default configlets during migration has the following conditions:

- 13.1 to 13.3:
 - Default Configlets are added if an entity with the same name does not exist in 13.1.
 - Default Configlets are over written if an entity with the same name exists in 13.1.
- 13.3 to later releases:

- Default Configlets are not added/overwritten, if the default Configlet is modified/deleted by the user in 13.3.

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 to 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 to 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 to 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 value from 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 FPCs belonging to a device and certain configuration only on the first FPC 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 from 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 in 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 param 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
```

}

Parameter	Details
\$INTERFACENAME	<p>A variable with an XPath configured to fetch all the interface names.</p> <p>Configured Value XPath: //device/interface-information/physical-interface/name/text()</p>



NOTE: When using \$INTERFACE, \$UNIT, Configured Value Xpath, Invisible Params, Selection fields; the variable definition in the configlet editor should contain .get(0) in order in order to fetch the value from the array. Eg: \$INTERFACE.get(0)

- Related Documentation**
- [CLI Configlets Overview on page 215](#)
 - [Viewing CLI Configlet Statistics](#)

CHAPTER 24

Configuration Views Overview

- [Configuration Views Overview on page 243](#)
- [Configuration View Variables on page 244](#)
- [Configuration View Workflow on page 244](#)
- [Configuration Views User Roles on page 246](#)
- [XML Extensions on page 246](#)

Configuration Views 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. The four types of configuration views are Form View, Grid View, XML View, and CLI View. Form View is simple view of configuration as key value pair. The dynamic fields in form view are defined using parameters. Grid view is 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. XML and CLI views show the configuration XML and CLI format of the selected component.

Configuration Views Workspace can be accessed by selecting **Configlets > Configuration Views** from the Junos Space user interface. You can perform the following tasks from **Configlets > Configuration Views**.

- 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 CLI Configlets 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

- [Deleting Configuration Views on page 251](#)
- [Default Configuration Views Examples on page 252](#)

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/releases/velocity-1.4/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**
- [Modifying a Configuration View on page 251](#)

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 views with the same name.
Domain	Domain to which the configuration view is associated
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. The order can accept values from 1 to 65535.
View Type	View types are Form View, Grid View, XML View, and CLI View..

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.

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 • [Configuration Views Overview on page 243](#)

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 **Network Management Platform > Role Based Access Control > Users**. The 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

- [Modifying a Configuration View on page 251](#)

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**

- [Modifying a Configuration View on page 251](#)

Managing Configuration Views

- [Creating a Configuration View on page 249](#)
- [Modifying a Configuration View on page 251](#)
- [Deleting Configuration Views on page 251](#)
- [Viewing Configuration Views Statistics on page 252](#)
- [Default Configuration Views Examples on page 252](#)

Creating a Configuration View

You create a configuration view from the Configlets workspace.

To create a configuration view:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View**.

The Configuration View page is displayed.

2. Click the Create Configuration View icon from the Actions menu.

The Create Configuration View page is displayed. [Table 30 on page 249](#) lists the columns displayed on this page.

Table 30: Configuration Views Page Columns

Field	Description
Name	Name of the configuration view
Domain	Domain to which the configuration view is associated
Title	Title of the configuration view
Device Family	Family of the device
Description	Description of the configuration view
Order	Order in which the view has to be applied and it accepts only values greater than zero
View Type	Type of configuration view - Form view, Grid view, XML view, and CLI view

Table 30: Configuration Views Page Columns (*continued*)

Field	Description
Creation Time	Date and time when the configuration view was created
Last Updated Time	Latest time when the configuration view was last updated
Last Modified By	Login ID of the user who last modified the configuration view

3. In the **Name** field, enter the name for 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 views with the same name.

4. From the **View Type** drop-down list, select the type of configuration view you want to create.

5. In the **Title** field, enter a title for the configuration view.

The title cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).

6. From the **Device Family Series** drop-down list, select the appropriate device family for which you want to create a configuration filter.

7. From the **Context** drop-down list, select the appropriate xpath.

8. (Optional) In the **Description** field, enter a description.

The description cannot exceed 2500 characters.

9. In the **Order** field, enter an appropriate value.

10. Click the Add Parameter icon to add a parameter.

The Add Form View Parameter pop-up window is displayed. Configure the parameter on this page.

- a. In the **Parameter** field, enter the name of the parameter.
 - b. In the **Display Name** field, enter a display name for this parameter.
 - c. Select the **Script Dependant** check-box if you want to use a script.
 - If you select the configuration view to depend on a script, select the appropriate local script from the **Local Script** drop-down list.
 - d. From the **Configured Value Xpath** drop-down list, select an appropriate xpath value.
 - e. In the **Order** field, enter an appropriate value.
 - f. Click **Add**.
11. (Optional) Add multiple parameters.
 12. Click **Create**.

The configuration view is created.



NOTE: To assign a configuration view to a domain, select the configuration view and select **Assign Configuration View to Domain** from the Actions menu.

Related Documentation

- [Configuration Views Overview on page 243](#)
- [Modifying a Configuration View on page 251](#)

Modifying a Configuration View

You modify a configuration view when you want to change the properties of the configuration view.

To modify a configuration view:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View**.

The Configuration View page is displayed.

2. Select the configuration view you want to modify and select the Modify Configuration View icon on the Actions menu.

The Modify Configuration View page is displayed.

3. Modify the properties of the configuration view and click **Update**.

The configuration view is modified.

Related Documentation

- [Configuration Views Overview on page 243](#)
- [Creating a Configuration View on page 249](#)

Deleting Configuration Views

You delete configurations view when want to remove it from Junos Space Network Management Platform.

To delete configuration views:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View**.

The Configuration View page is displayed.

2. Select the configurations views you want to delete and select the Delete Configuration View icon from the Actions menu.

The Delete Configuration View pop-up window is displayed.

3. Click **Delete**.

The configuration views are deleted.

- Related Documentation**
- [Configuration Views Overview on page 243](#)
 - [Creating a Configuration View on page 249](#)

Viewing Configuration Views Statistics

You can view the statistics about the configuration views from the CLI Configlets workspace. The Configuration Views landing page displays the Configuration Viewer Count by Device Family bar chart. The bar chart shows the number of configuration views on the y axis and device family series on the x axis.

To view the statistics of configuration views:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets**.

The CLI Configlets landing page is displayed. This page displays the charts related to CLI configlets and configuration views.

2. Click the Configuration Viewer Count by Device Family chart.

You will be redirected to the Configuration Views page.

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.

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**
- [Modifying a Configuration View on page 251](#)

Default Configuration Views Examples

Default configuration Views are added during server start up or data migration during an upgrade. These default configuration Views are added only on the initial server start up and data migration during an upgrade. Default configuration Views cannot be added every time the server starts. The user can perform all the usual operations with the default configuration Views including delete operation.

Adding default configuration Views during migration has the following conditions:

- 13.1 to 13.3:
 - Default configuration Views are added if an entity with the same name does not exist in 13.1.
 - Default configuration Views are over written if an entity with the same name exists in 13.1.
- 13.3 to later releases:

- Default configuration Views are not added/overwritten, if the default configuration Views is modified/deleted by the user in 13.3.

Default view

This view produces the configuration of the selected node in CLI format- curly brace format.

Context: //

This configuration view is targeted for all the entities.

Sample CLI view

```
## Device: EX4200

interfaces {
  ge-0/0/4 {
    description "desc";
    unit 0 {
      description "description for Unit;";
    }
  }
}
```

Example XML view

This view produces the configuration of the selected node in XML format.

Context: ///device/configuration/protocols

This configuration view is targeted for protocols.

Sample CLI view

```
## Device: EX4200

<!-- Device: Ex4200 -->
<protocols>
  <igmp-snooping>
    <vlan>
      <name>all</name>
    </vlan>
  </igmp-snooping>
  <rstp>
  </rstp>
  <lldp>
    <interface>
      <name>all</name>
    </interface>
  </lldp>
  <lldp-med>
    <interface>
      <name>all</name>
    </interface>
```

```
</lldp-med>
</protocols>
```

Example Form view

This form view displays certain important information about device.

Context:/device

Sample Form view Details:

Table 31: Parameters

Display name	Script dependent	Parameter	Configured value xpath	Order
Device Name	false	Device_Name	/device/system-information/host-name/text()	1
OS Version	false	OS_Version	/device/system-information/os-version/text()	2
Serial Number	false	Serial_Number	/device/system-information/serial-number/text()	3
Chassis	false	chassis_description	/device/chassis-inventory/chassis/description/text()	4
Location	false	snmp_location	/device/configuration/snmp/location/text()	5
Contact	false	snmp_contact	/device/configuration/snmp/contact/text()	6

Sample Form View:

Device Name: ACX-34

OS Version: 12.3-20130818_att_12q3_x51.0

Serial Number: ABCDE12345

Chassis: ACX1100

Location: location1

Contact: John Doe

Example Form view

This view displays information about the selected node in Grid format.

Context:/device

Sample Grid View Details

Table 32: Parameters

Parameter	Index parameter	Display name	Script dependent	Customized attribute	Editable	Order
Device_Name	true	Device Name	false	false	false	1
Physical_Interface_Name	true	Physical Interface Name	false	false	false	2
IP_Address	false	IP Address	false	false	false	3
MAC_Address	false	MAC Address	false	false	false	4
Operational_Status	false	OperationalStatus	false	false	false	5
Admin_Status	false	Admin Status	false	false	false	6
Speed	false	Speed	false	false	false	7

Table 33: Parameters and Configured Value Xpath

Parameter	Configured value xpath	Order
Device_Name	/device/system-information/host-name/text()	1
Physical_Interface_Name	/device[name='\$Device_Name']/interface-information/physical-interface [starts-with(name,'xe')or starts-with(name,'ge-')or starts-with(name,'fe')]/name/ text()	2
IP_Address	/device[name='\$Device_Name']/configuration/interfaces/interface [name='\$Physical_Interface_Name']/unit[name='0'] /family/inet/address/name/text()	3
MAC_Address	device[name='\$Device_Name']/interface-information/physical-interface [name='\$Physical_Interface_Name']/hardware-physical-address	4
Operational_Status	/device[name='\$Device_Name']/interface-information/physical-interface [name='\$Physical_Interface_Name']/oper-status/text()	5
Admin_Status	/device[name='\$Device_Name']/interface-information/physical-interface [name='\$Physical_Interface_Name']/admin-status/text()	6
Speed	/device[name='\$Device_Name']/interface-information/physical-interface [name='\$Physical_Interface_Name']/speed/text()	7

Sample Grid View

Device Name	Physical interface	IP address	MAC address	Operational status	Admin status	Speed
ACX-34	ge-0/0/0		00:00:5E:00:53:00	down	Up	1000mbps
ACX-34	ge-0/0/1		00:00:5E:00:53:00	down	Up	1000mbps

Device Name	Physical interface	IP address	MAC address	Operational status	Admin status	Speed
ACX-34	ge-0/0/2		00:00:5E:00:53:00	down	Up	1000mbps
ACX-34	ge-0/0/3		00:00:5E:00:53:00	down	Up	1000mbps

Related Documentation • [CLI Configlets Overview on page 215](#)

CHAPTER 26

XPath and Regex

- [XPath and Regex Overview on page 257](#)
- [Creating Xpath or Regex on page 257](#)
- [Modifying Xpath and Regex on page 258](#)
- [Deleting Xpath and Regex on page 258](#)
- [XPath and Regular Expression Examples on page 259](#)

XPATH and Regex Overview

While developing configlets, XPath and Regular Expressions would be used intensively. It would be desirable to let the user define frequently used XPath 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 or Regex on page 257](#)

Creating Xpath or Regex

You create Xpath and Regex from the CLI configlets workspace.

To create an Xpath and Regex:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Xpath and Regex**.

The Xpath and Regex page is displayed.

2. Click the Create Xpath and Regex icon on the Actions menu.

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**.

The Xpath or regular expression is created.



NOTE: To assign the Xpath or regular expression to a domain, select **Assign Xpath to Domain** from the the Actions menu.

**Related
Documentation**

- [XPATH and Regex Overview on page 257](#)

Modifying Xpath and Regex

You modify an Xpath and Regex when you want to change the properties of the Xpath or Regex.

To modify an Xpath and Regex:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Xpath and Regex**.

The Xpath and Regex page is displayed.

2. Select the Xpath and Regex you want to modify and select the Modify Xpath and Regex icon on the Actions menu.

The Modify Xpath/Regex page is displayed.

3. Modify the Xpath and Regex properties and click **Update**.

The Xpath and Regex is modified.

**Related
Documentation**

- [XPATH and Regex Overview on page 257](#)
- [Creating Xpath or Regex on page 257](#)

Deleting Xpath and Regex

You delete an Xpath and Regex when you no longer want it on Junos Space Network Management Platform.

To delete an Xpath and Regex:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Xpath and Regex**.

The Xpath and Regex page is displayed.

2. Select the Xpath and Regex you want to delete and select the Delete Xpath and Regex icon on the Actions menu.

The Delete Xpath/Regex pop-up window is displayed.

3. Click **Delete**.

The Xpath and Regex is deleted.

- Related Documentation**
- [XPATh and Regex Overview on page 257](#)
 - [Creating Xpath or Regex on page 257](#)

XPath and Regular Expression Examples

Default Xpath and Regex are added during server start up or data migration performed during an upgrade. These default Xpath and Regex are added only on the initial server start up and during data migration as a result of an upgrade. The User can perform all the usual operations on the default Xpath and Regex, including delete operation.

Adding default Xpath and Regex during migration has the following conditions:

- 13.1 to 13.3:
 - Default Xpath and Regex are added if an entity with the same name does not exist in 13.1.
 - Default Xpath and Regex are over written if an entity with the same name exists in 13.1.
- 13.3 to later releases:
 - Default Xpath and Regex are not added/overwritten, if the default Xpath and Regex is modified/deleted by the user in 13.3.

Example 1 – Alphanumeric

To refer in configlet's Regex Value. It accepts all the alphanumeric characters.

Type: Regular Expression

Value: [a-zA-Z0-9]*

Example 2 - Logical Interfaces per Physical Interface

To fetch the logical interface of selected physical interface

Type: Xpath Context

Value:

/device/configuration/interfaces/interface[name="\$INTERFACE.get(0)"]/unit/name/text()

Example 3 – Physical Interfaces

To fetch the name of the physical interface

Type: Xpath Context

Value: /device/interface-information/physical-interface/name/text()

Example 4 – Devices

To fetch the name of the selected device

Type: Xpath Context

Value: /device/name/text()

- Related Documentation**
- [XPath and Regex Overview on page 257](#)
 - [Creating Xpath or Regex on page 257](#)

CHAPTER 27

Configuration Filter

- [Creating a Configuration Filter on page 261](#)
- [Modifying a Configuration Filter on page 262](#)
- [Deleting Configuration Filters on page 262](#)

Creating a Configuration Filter

Configuration Filters restrict the scope of the configuration nodes and options displayed in the View Device Configuration page in the Devices workspace. You can create configuration filters for a specific device family in the CLI Configlets workspace. These configuration filters are available in the device configuration page when you configure the device. You can choose these configuration filters in the left pane on the device configuration page.

To create a configuration filter:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration Filter**.

The Configuration Filter page is displayed.

2. Click the Add Configuration Filter icon on the Actions menu.

The Add Configuration Filter page is displayed.

3. Select **Device Configuration > View Active Configuration** from the Actions menu.

The Device Configuration View page is displayed.

4. Click the Create Filter icon in the left pane of the Device Configuration page.

The Add Configuration Filter pop-up window is displayed.

5. In the **Name** box, enter a user-defined configuration filter name.

6. Select the appropriate device family from the **Device Family** drop-down list.

7. Select the configuration nodes on the left and click **Create**.

The configuration view is created.

Related Documentation

- [Configuration Filter](#)
[Modifying a Configuration Filter on page 262](#)

Modifying a Configuration Filter

You modify a configuration filter when you want to change the properties of the configuration filter.

To modify a configuration filter:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration Filter**.

The Configuration Filter page is displayed.

2. Select the configuration filter you want to modify and select the Modify Configuration Filter icon on the Actions menu.

The Modify Configuration Filter page is displayed.

3. Modify the properties of the configuration filter and click **Update**.

The configuration filter is modified.

Related Documentation

- [Creating a Configuration Filter on page 261](#)
- [Deleting Configuration Filters on page 262](#)

Deleting Configuration Filters

You delete configuration filters when you want to remove them from Junos Space Network Management Platform

To delete a configuration filter:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration Filter**.

The Configuration Filter page is displayed.

2. Select the configuration filters you want to delete and select the Delete CLI Configlet icon from the Actions menu.

The Delete Configuration Filter pop-up window is displayed.

3. Click **Confirm**.

The configuration filters are deleted.

Related Documentation

- [Creating a Configuration Filter on page 261](#)

PART 5

Images and Scripts

- [Overview on page 265](#)
- [Device Images on page 273](#)
- [Scripts on page 275](#)
- [Operations on page 281](#)
- [Script Bundles on page 283](#)
- [Configuration: Device Images on page 285](#)
- [Configuration: Scripts on page 311](#)
- [Configuration: Operations on page 337](#)
- [Configuration: Script Bundles on page 347](#)
- [Administration: Scripts on page 359](#)
- [Administration: Operations on page 363](#)
- [Administration: Script Bundles on page 365](#)
- [Annotations and Examples on page 367](#)

CHAPTER 28

Overview

- [Device Images and Scripts Overview on page 265](#)

Device Images and Scripts Overview

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade to or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

Images and Scripts is a workspace in 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 Junos Space Network Management Platform user interface.

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 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, or execute them on those devices.

- Manage operations.

You create, manage, export, import, and execute operations that combine multiple scripts 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 administrator to create users and control their access to different tasks, it also has a set of predefined user roles. [Table 34 on page 266](#) describes the Images and Scripts tasks to which different users have access, based on the roles the administrator assigns to them (for the latest list of permitted tasks for each role, see **Role Based Access Control > Roles > Select the role > View Detail** on the Junos Space Network Management Platform user interface).

You can create users and manage them on the Users page, if you have User Administrator permissions. To create and manage these users, select **Role Based Access Control > User Accounts** on the Junos Space Network Management Platform user interface. The User Accounts page lists the existing users. To create and assign roles to Images and Scripts users, see [“Creating User Accounts” on page 571](#).

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 34: Images and Scripts User Roles

User Role	Permitted Tasks
For Device Images	

Table 34: Images and Scripts User Roles (*continued*)

User Role	Permitted Tasks
Device Image Manager	<p>For devices:</p> <ul style="list-style-type: none"> • Add Adapter • Upgrade Adapter • Delete Adapter <p>For images and scripts:</p> <ul style="list-style-type: none"> • Import Images • View Deployed Results • Modify Device Image • Delete Device Images • Stage Image on Device • MD5 Validation Result • Verify Image on Devices • Deploy Device Image • Remove Image from Staged Device • View Associated Devices • Assign Image to Domain
Device Images Read Only User	<p>For images:</p> <ul style="list-style-type: none"> • View Deployed Results • View Associated Devices
For Scripts	

Table 34: Images and Scripts User Roles (*continued*)

User Role	Permitted Tasks
Device Script Manager	<p>For devices:</p> <ul style="list-style-type: none"> • View Script Executions <p>For images and scripts:</p> <ul style="list-style-type: none"> • Compare Script Versions • Import Script • View Execution Results • Modify Script • Modify and Stage Scripts on Device • 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 • Assign Script to Domain <p>For script bundles:</p> <ul style="list-style-type: none"> • Create Script Bundle • Embedded Script • Modify Script Bundle • Delete Script Bundles • Stage Script bundle on Devices • View Associated Devices • Enable Script Bundle on Devices • Disable Script Bundle on Devices • Execute sScript Bundle on Devices
Device Script Operator	<p>For devices:</p> <ul style="list-style-type: none"> • Device Management • Secure Console <p>For images and scripts:</p> <ul style="list-style-type: none"> • Scripts <ul style="list-style-type: none"> • Compare Script Versions • Execute Script on Devices

Table 34: Images and Scripts User Roles (*continued*)

User Role	Permitted Tasks
Device Script Read Only User	<p>For images and scripts:</p> <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
For Operations	

Table 34: Images and Scripts User Roles (*continued*)

User Role	Permitted Tasks
Operation Manager	

Table 34: Images and Scripts User Roles (*continued*)

User Role	Permitted Tasks
	<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 • View Script Executions • Images and Scripts <ul style="list-style-type: none"> • Images <ul style="list-style-type: none"> • Import Images • View Deployed Results • Modify Device Image • Delete Device Images • Stage Image on Device • MD5 Validation Result • Verify Image on Devices • Deploy Device Image • Remove Image from Staged Device • View Associated Devices • Assign Image to Domain • Scripts <ul style="list-style-type: none"> • Compare Script Versions • Import Script • View Execution Results • Modify Script • Modify and Stage Scripts on Device • 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 • Assign Script to Domain • Script Bundles <ul style="list-style-type: none"> • Create Script Bundle • Embedded Script • Modify Script Bundle • View Associated Devices • Enable Script Bundle on Devices • Disable Script Bundle on Devices

Table 34: Images and Scripts User Roles (*continued*)

User Role	Permitted Tasks
	<ul style="list-style-type: none">• Delete Script Bundles• Stage Script Bundle on Devices• Execute Script Bundle on Devices• Assign Script Bundle to Domain• Operations<ul style="list-style-type: none">• Create Operation• Clone Operation• Modify Operation• Delete Operations• Import Operations• Export Operations• Run Operation• View Operation Results• Assign Operation to Domain

-
- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Operations Overview on page 281](#)
 - [Scripts Overview on page 275](#)
 - [Script Bundles Overview on page 283](#)

CHAPTER 29

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 to or downgrade from one Junos operating system (Junos OS) release to another. You can download device images from <https://www.juniper.net/customers/support/>. For more information about downloading device images, see the *Junos OS Installation and Upgrade Guide*.

Junos Space Network Management Platform facilitates the management of device images for devices running Junos OS by enabling you to upload device images from your local file system and deploy them onto a device or 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 you upload a device image, you can stage the 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 a device image.

Based on the user role assigned to your username, Junos Space Network Management Platform enables or disables different tasks. For more information about the roles that you need to be able to perform tasks on device images, see “[Device Images and Scripts Overview](#)” on page 265.

[Table 35 on page 273](#) describes the Images page. You can use the filter functionality on the **File Name**, **Domain**, and **Version** drop-down lists to specify the filter criteria. When you apply the filters, the table displays only the values that match the filter criteria. The **Series**, and **Associations** fields, however, do not support the filter option.

Table 35: Images Page

Field	Description
File Name	Name of the device image For example, jinstall-ex-4200-12.3R4.6-domestic-signed.tgz.

Table 35: Images Page (*continued*)

Field	Description
Version	Version of the device image For example, 12.3R4.6.
Series	Series supported by the device image For example, EX4200.
Associations	Click View in this column to view the devices on which this image is deployed.
Domain	Domain to which this image belongs. By default, the image belongs to the global domain.

You can perform the following tasks from the Images page:

- Upload device images onto Junos Space Network Management Platform.
- View details of the image uploaded to Junos Space Network Management Platform.
- Modify a device image.
- Delete device images from both Junos Space Network Management Platform and devices.
- View device image deployment results.
- Deploy a device image.
- Stage a device image onto a device.
- View the devices that are associated with a staged image.
- View and delete MD5 validation results.
- Verify the checksum.
- Tag and untag the images, view the images that are tagged, and delete private tags.
- Clear the selected images.

**Related
Documentation**

- [Deploying Device Images on page 293](#)
- [Staging Device Images on page 286](#)
- [Modifying Device Image Details on page 307](#)
- [Uploading Device Images to Junos Space on page 285](#)
- [Scripts Overview on page 275](#)
- [Script Bundles Overview on page 283](#)
- [Operations Overview on page 281](#)

CHAPTER 30

Scripts

- [Scripts Overview on page 275](#)
- [Promoting Scripts Overview on page 279](#)

Scripts Overview

Scripts are configuration and diagnostic automation tools provided by the Junos Operating System (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 to 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 correct 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. Then, 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, or 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 with devices. It maintains this association with 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 or 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 associated devices
- Autoupgrading 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, or execute scripts— but you cannot 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 it is associated with a device. You need to first remove the scripts from the device and then modify the script type.

Based on the user role assigned to your username, Junos Space Network Management Platform enables or disables different tasks. For more information about the roles that you need to be able to perform any tasks on scripts, see [“Device Images and Scripts Overview” on page 265](#).

[Table 36 on page 276](#) describes the information that appears on the Scripts page.

You can use the filter option on the **Script Name**, **Domain**, **Descriptive Name**, **Type**, **Execution Type**, **Format**, and **Latest Revision** drop-down lists to specify the filter criteria. When you apply the filters, the table displays only the values that match the filter criteria. The **Description**, **Creation Date**, **Last Updated Time**, and **Associations** fields do not support the filter option.

Table 36: Scripts Page Fields Description

Field	Description
Script Name	Name of the script file

Table 36: Scripts Page Fields Description (*continued*)

Field	Description
Domain	Domain to which the script belongs
Descriptive Name	Descriptive name of the script
Type	Type of script: <ul style="list-style-type: none"> • Commit Script • Op Script • Event Script
Execution Type	<ul style="list-style-type: none"> • Device—Scripts of this type need to be staged and enabled on a device before the scripts can be executed. • Local—Scripts of this type need not be staged or enabled on a device for the scripts to be executed. You must set the @ISLOCAL annotation to true to execute the script locally. For more information about script annotations and a sample script, see “Scripts Annotations” on page 367 and “Script Example” on page 371.
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.
Description	Description of the script
Last Updated Time	Latest time when the script was last updated
Associations	Associated devices for a script that are displayed when you click View in the Associations column

You can perform the following tasks from the Scripts page:

- Import scripts.
- View script details.
- Modify a script.
- Delete scripts.
- Disable scripts on devices.
- Enable scripts on devices.
- Execute a script on devices.
- Remove scripts from devices.
- Stage scripts on devices.
- Compare script versions.

- Export scripts in .tar format.
- Modify the type of script.
- View associated devices.
- View verification results.
- Verify the checksum of scripts on devices.
- View execution results.
- Tag and untag the scripts, view the scripts that are tagged, and delete private tags.
- Unselect scripts that you had previously selected.

To help get you started, Juniper Networks provides you with a few sample scripts that you can download and customize to suit your requirements. Commit, event, and op sample scripts are stored in the script library.

To access the sample scripts:

1. In a browser window, type the following URL:
<http://www.juniper.net/in/en/community/junos/script-automation/library/>
The Script Library page appears.
2. Click the **Configuration Automation**, **Event Automation**, or **Operations Automation** link to access the commit, event, or op sample scripts respectively.
The corresponding HTML page listing the sample scripts appears for the chosen script category.
3. Click a sample script to view its details.
If you are using Internet Explorer (IE), you are provided with an option to save the script onto your local system. After you download the script, open it using an editor such as Notepad.
If you are using browsers other than IE, you can download the script by clicking the script link provided under the **Source** section in the browser window displaying the script. After you download the script, open it using an editor such as Notepad.

To run any of your scripts on devices, see [“Executing Scripts on Devices” on page 331](#) and [“Executing Scripts on Devices Locally with JUISE” on page 78](#).

Related Documentation

- [Device Images and Scripts Overview on page 265](#)
- [Importing Scripts on page 334](#)
- [Viewing Script Details on page 359](#)
- [Modifying a Script on page 311](#)
- [Modifying Script Types on page 314](#)
- [Comparing Script Versions on page 314](#)
- [Deleting Scripts on page 315](#)

- [Exporting Scripts in .tar Format on page 361](#)
- [Staging Scripts on Devices on page 316](#)
- [Viewing Execution Results on page 333](#)
- [Verifying the Checksum of Scripts on Devices on page 320](#)
- [Viewing Verification Results on page 360](#)
- [Enabling Scripts on Devices on page 321](#)
- [Disabling Scripts on Devices on page 324](#)
- [Removing Scripts from Devices on page 328](#)
- [Executing Scripts on Devices on page 331](#)
- [Device Images Overview on page 273](#)
- [Script Bundles Overview on page 283](#)
- [Operations Overview on page 281](#)
- [Viewing Device Association of Scripts on page 319](#)

Promoting Scripts Overview

Promote script feature empowers the user to create their own actions on a device, physical interface, logical interface and physical inventory component. It is a straight forward approach for executing a script as an action rather than executing the script from execute script window. Normally for example – if a user needs to reboot a device, the user selects a device -> Device operations -> Execute script, the Execute script window opens and then the user will select that particular script, provides required parameter and then execute the script. However in case of script promotion, the script will be made available as right click action, hence the user can select the device and execute the script in one click. The user need not open execute script window for executing script. The promote script feature eases the script execution process on device, interfaces and physical inventory.

Scripts can be promoted by including @PROMOTE annotation. It should have the value as 'yes'. `/*@PROMOTE="yes"*/`

A Device Script with @PROMOTE annotation needs to be staged and enabled for execution on the device. In case of a Device Script, if the promoted script is not staged and enabled it will appear as a disabled action but for interfaces and physical inventory components the promoted script will not appear at all if it is not staged and enabled.

Local scripts can also be promoted and are not subject to these restrictions.



.....

NOTE: The promote script feature works only when the option “Advanced Xpath processing” is enabled. The User can configure this option by going to **Administration > Applications > Modify Application Settings > CLIConfiglets**. Only OP scripts can be promoted. Script promotion does not support multiple selection.

.....

Related Documentation

- [Scripts Overview on page 275](#)

CHAPTER 31

Operations

- [Operations Overview on page 281](#)

Operations Overview

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade to 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 of tasks that are frequently performed.

Based on the user role assigned to your username, Junos Space Network Management Platform enables or disables different tasks. For more information about the roles that you need to be able to perform any tasks on operations, see [“Device Images and Scripts Overview” on page 265](#).

You can perform the following tasks from the Operations page:

- Create an operation.
- Modify an operation.
- Delete operations.
- Create a copy of an existing operation.
- Execute (or run) an operation.
- Export operations.
- Import an operation.
- View information about operations in four stages of execution (successful, failed, in progress, and scheduled).
- Tag and untag operations, view operations that are tagged, and delete private tags.

Related Documentation

- [Creating an Operation on page 337](#)

- [Modifying an Operation on page 340](#)
- [Running an Operation on page 341](#)
- [Copying an Operation on page 342](#)
- [Viewing Operations Results on page 363](#)
- [Deleting an Operation on page 343](#)
- [Exporting an Operation in .tar Format on page 344](#)
- [Importing an Operation on page 345](#)
- [Scripts Overview on page 275](#)
- [Device Images Overview on page 273](#)
- [Script Bundles Overview on page 283](#)

Script Bundles

- [Script Bundles Overview on page 283](#)

Script Bundles Overview

Scripts are configuration and diagnostic automation tools provided by the Junos Operating System (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 334](#)). 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 or disables different tasks. For more information about the roles that you need to perform any tasks on script bundles, see [“Device Images and Scripts Overview” on page 265](#).

You can execute the following tasks from the Script Bundles page:

- Create a script bundle.
- View details about a script bundle.
- Modify a script bundle.
- Delete script bundles.
- Execute script bundles on devices.
- Stage a script bundle on devices.
- View device association of scripts in script bundles.
- Enable scripts in a script bundle on devices.
- Disable scripts in a script bundle on devices.

- Deploy script bundles to devices.
- Tag and untag script bundles, view script bundles that are tagged, and delete private tags.

**Related
Documentation**

- [Creating a Script Bundle on page 347](#)
- [Staging Script Bundles on Devices on page 350](#)
- [Executing Script Bundles on Devices on page 353](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Enabling Scripts in Script Bundles on Devices on page 355](#)
- [Disabling Scripts in Script Bundles on Devices on page 356](#)
- [Viewing Device Associations of Scripts in Script Bundles on page 365](#)
- [Device Images Overview on page 273](#)
- [Scripts Overview on page 275](#)
- [Operations Overview on page 281](#)

Configuration: Device Images

- [Uploading Device Images to Junos Space on page 285](#)
- [Staging Device Images on page 286](#)
- [Viewing Device Association of Images on page 289](#)
- [Verifying the Checksum on page 290](#)
- [Deploying Device Images on page 293](#)
- [Viewing Device Image Deployment Results on page 302](#)
- [Deleting Device Images on page 303](#)
- [Modifying Device Image Details on page 307](#)
- [Viewing and Deleting MD5 Validation Results on page 308](#)

Uploading Device Images to Junos Space

To deploy a device image using Junos Space Network Management Platform, you must first download the device image from the Juniper Networks Support webpage <http://www.juniper.net/customers/support/>. Save the downloaded 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 device image is uploaded, you can stage the 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 and from the devices to which you have deployed the device image.

To upload device images to Junos Space Network Management Platform:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Click the **Import Image** icon.

The Import Images page appears.

3. Click **Browse**.

The File Upload dialog box displays the directories and folders on your local file system.

4. Navigate to the device image file and click **Open**.
5. 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 Junos Space server, it is listed on the Images page.

**Related
Documentation**

- [Staging Device Images on page 286](#)
- [Verifying the Checksum on page 290](#)
- [Deploying Device Images on page 293](#)
- [Device Images Overview on page 273](#)

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 is transferred completely.

To stage a device image on devices:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Select the device image and select **Stage Image on Device**. The Stage Image on Devices page appears. The devices that are listed belong to the device family that supports this image.

This page displays the following information:

- **Image name**—Name of the image that you have selected for staging
- **MD5 Value**—32-character hexadecimal number that is computed on the selected device image file, which is stored on the Junos Space server
- **Device Name**—Name of the discovered device, which is an identifier used for network communication between Junos Space Network Management Platform and the Junos OS device.
- **IP Address**—IP address of the discovered device. For example, 10.1.1.1.
- **Platform**—Platform of the discovered device. For example, MX480.
- **Software Version**—Operating system firmware version running on the device. For example, 13.1X49D29.1.

- **Staged Status**—Indicates whether the selected image is staged on the discovered device. This column displays either **Staged** (if the image is staged) or **Not Staged** (if the image is not yet staged).
- **Checksum Status**—Indicates whether the device image on the Junos Space server and the device are the same:
 - **Valid** means that the checksum values of the device image on the Junos Space server and the device match.
 - **Invalid** means that the checksum values do not match.
 - **NA** means that the selected image is not staged on the device yet.

You may want to stage an image whose checksum status is “Invalid” because this action might stage the correct image onto the device, thereby making the checksum status “Valid.” You can deploy an image only when the checksum status is “Valid.”

- **Last Checksum Time**—Time when the checksum was last verified. For a device in which the selected image is not staged yet, this column displays **NA**.

A user verifies the checksum manually by selecting the **Verify Image on Devices** option on the Junos Space GUI.

You can sort the data displayed in the following columns: **Device Name**, **IP Address**, **Platform**, **Software Version**, **Staged Status**, **Checksum Status**, and **Last Checksum Time**.

You can filter the data displayed in the following columns: **Device Name**, **IP Address**, **Platform**, and **Software Version**.

3. Select the device or devices on which you want to stage the device image by using one of the following selection modes—manually, on the basis of tags, or by using a CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select Device Manually** option is selected and the complete list of devices is displayed.

To select devices manually:

- a. Click the **Select Device Manually** option, if it is not selected previously.
- b. Select the devices on which you want to stage the device image.

The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

- c. To select all devices, select the check box in the column header next to **Device Name**.

To select devices on the basis of 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, displaying two categories of tags—Public and Private.

- c. 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.

To search for a specific tag, enter the first few letters of the tag name 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.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices by using a CSV file:

- a. Select the **Select by CSV** option.
- b. Click **Browse** and upload the file in .XLS format containing the list of devices on which you want to deploy the device image.



TIP: For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

4. (Optional) To remove any existing device images from the device, expand the **Staging Options** section and select the **Delete any existing image before download** check box. This selection deletes all .tgz files and files whose filenames begin with **jinstall**.

When you delete a previously staged image, an audit log entry is automatically generated.

5. (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.
6. Click **Stage Image**.

The image is staged on the selected device or devices and an alert appears, displaying the job ID. However, if the devices on which you are trying to stage the device image does not have sufficient space to accommodate the image, then Junos Space throws an error message and the staging job fails.



NOTE: The time taken to stage an image depends on the size of the image, network connectivity, and the number of devices on which the image is staged. You can monitor the progress of completion from the **Percent** column on the **Job Management** page.

To verify whether the image is staged successfully, click the job ID link or navigate to the **Job Management** page and view the status of the job. If the job is a failure, you

can double-click the job to view the reason for failure. The Device Image Action Details page appears, which displays the reason for failure in the **Description** column. However, if the image is staged successfully, then this column displays:

Image jinstall-11.4R9.4-domestic-signed.tgz transferred successfully.

Also, you can export the information on the Device Image Action Details page as a comma-separated values (CSV) file.

To export data on the Device Image Action Details page as a CSV file:

- a. Click **Export as CSV**.

You are prompted to save the file.

- b. Click **OK** on the File Save dialog box to save the file to your local file system.

- c. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the staging of images failed.

You may want to verify the checksum of the staged device image to ensure that the image is transferred completely to the device. For more information about how to verify the checksum, see [“Verifying the Checksum” on page 290](#).

Related Documentation

- [Device Images Overview on page 273](#)
- [Deploying Device Images on page 293](#)
- [Verifying the Checksum on page 290](#)

Viewing Device Association of Images

You can view the images that are staged to a Junos device or devices by using Junos Space Network Management Platform. You can view the image–device association from the Images landing page by selecting one or more images. On the Images page, click **View** in the **Associations** column to view the associated devices for a single image.

To view devices on which an image is staged:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Select an image.



NOTE: Junos Space does not display images that are staged out-of-band.

3. Select **View Associated Devices** from the Actions menu.

The View Associated Devices page appears with valid image device association details, which includes the device name, IP address, platform, and software version of the devices. This page is read-only and hence you cannot perform any actions on this page.



NOTE: The image(–)device(s) association details are displayed only if you stage an image on to devices in Junos Space Release 13.3R1 or later versions. If you staged an image on to a device by using a version prior to Junos Space Release 13.3R1 and then upgraded to Release 13.3R1 or later versions, then this image(–)device(s) association is not displayed.

4. Click **Back** at the top of the View Associated Devices page to return to the Images page.

**Related
Documentation**

- [Deploying Device Images on page 293](#)
- [Staging Device Images on page 286](#)
- [Device Images Overview on page 273](#)

Verifying the Checksum

When you stage an image on a device using Junos Space Network Management Platform, sometimes the device image might not be completely transferred to the device. Verifying the checksum helps validate that the device image has been staged properly and is not corrupted or altered in any way from the device image that you staged from the Junos Space server.

The checksum value is a 32-character hexadecimal number that is computed on a file. If the checksum values of the device image file stored on the Junos Space server and the device match, then there is a high probability that the two files are the same.

To verify the checksum:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Select the image whose checksum you want to verify.
3. Select **Verify Image on Devices** from the Actions menu.

If this option is disabled (grayed out), one of the reasons could be that you have selected multiple images for verifying the checksum. Select only one image and repeat this step.

The Verifying checksum of image on device(s) dialog box appears. This page displays the following information:

- **Image name**—Name of the image, which you have selected for verifying the checksum
 - **MD5 Value**—32-character hexadecimal number that is computed on the selected device image file, which is stored on the Junos Space server
 - **Host Name**—Name of the discovered device, which is an identifier used for network communication between Junos Space Network Management Platform and the Junos OS device.
 - **IP Address**—IP address of the discovered device. For example, 10.1.1.1.
 - **Platform**—Platform of the discovered device. For example, MX480.
 - **Software Version**—Operating system firmware version running on the device. For example, 13.1X49D29.1.
 - **Staged Status**—Indicates whether the selected image is staged on the discovered device. This column displays either **Staged** (if the image is staged) or **Not Staged** (if the image is not yet staged).
 - **Checksum Status**—Indicates whether the device image on the Junos Space server and the device are the same:
 - **Valid** means that the checksum values of the device image on the Junos Space server and the device match.
 - **Invalid** means that the checksum values of the device image on the Junos Space server and the device do not match.
 - **NA** means that the selected image is not staged on the device yet.
 - **Last Checksum Time**—Time when the checksum was last verified. For a device in which the selected image is not staged yet, this column displays **NA**. This column is updated when an image is restaged on to the device.
4. Select the devices that have the device image staged on them by using one of the following selection modes—manually, on the basis of tags, or by using a CSV file. These options are mutually exclusive. If you select one, the others are disabled.



TIP: Perform a validation on those devices where the **Checksum Status** column shows **Valid** but the **Last Checksum Time** column displays a time that is way past the current time. By performing this action, you ensure that the image on the devices is valid currently.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

To select devices manually:

- a. Click the **Select Device Manually** option, if it is not selected previously.
- b. Select the devices on which you want to verify the checksum.

The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

- c. To select all devices, select the check box in the column header next to Host Name.

To select devices on the basis of 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, displaying two categories of tags—Public and Private.
- c. 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.

To search for a specific tag, enter the first few letters of the tag name 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.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices by using a CSV file:

- a. Select the **Select by CSV** option.
- b. Click **Browse** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.



TIP: For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application such as Microsoft Excel.

5. (Optional) To schedule a time for verifying the checksum, select the **Schedule at a later time** check box and use the lists to specify the date and time.
6. Click **Verify**.

The checksum value of the device image file on the Junos Space server is validated against the checksum value of the device image file stored on the selected devices. An alert appears, displaying the job ID.

To verify the devices on which the checksum status is valid, click the job ID link or navigate to the Job Management page and view the status of the job. If the job is a success, then the checksum values match on all devices selected for verification. However, if the job is a failure, double-click the job to identify the devices on which this job is a failure. The Device Image Action Details displays the reason for failure in

the **Description** column. Validation may fail if the checksum values do not match and for other reasons such as when the image is not staged on the device. To confirm, check the **Checksum Status** column value for the device by using **Images and Scripts > Images > Select the image > Verify Image on Devices** or from the Deploy Device Image inventory landing page.

Also, you can export information from the Device Image Action Details page as a CSV file to your local system.

To export data from the Device Image Action Details page to your local system:

- a. Click **Export as CSV**.

You are prompted to save the file.

- b. Click **OK** on the File Save dialog box to save the file to your local file system.

- c. After you save the file, to return to the Job Management page, click OK on the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the image verification failed.

When you verify a checksum, an audit log entry is automatically generated.

- Related Documentation**
- [Device Images Overview on page 273](#)
 - [Deploying Device Images on page 293](#)

Deploying Device Images

Junos Space Network Management Platform enables you to deploy device images onto a device or 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 perform a unified in-service software upgrade (ISSU) between two different Junos OS 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 unified 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 37 on page 294 describes the devices and software releases that support unified ISSU.

Table 37: 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 performing a unified 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 unified ISSU on an MX Series device, you must manually configure the device to enable **Non-stop bridging**, in addition to GRES and NSR that Junos Space enables on the dual Routing Engine device for unified 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 unified 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 Series 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 Routing Engine device, make sure that GRES and NSR are disabled on the device.

To deploy device images:

1. On the Junos Space Network Management Platform user interface, select **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 Devices page displays the devices that are supported by the selected device image. For a description of the fields in this table, see [Table 38 on page 296](#).

Table 38: Select Devices Table Field Descriptions

Field	Description
Image name	Name of the device image. (This field is above the devices table.)
MD5 Value	32-character hexadecimal number that is computed on the selected device image file, which is stored on the Junos Space server
Device Name	Identifier used for network communication between Junos Space Network Management Platform and the device running Junos OS.
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.
Staged Status	Indicates whether the selected image is staged on the discovered device. This column displays either Staged (if the image is staged) or Not Staged (if the image is not yet staged).
Checksum Status	Indicates whether the device image on the Junos Space server and the device are the same: <ul style="list-style-type: none"> • Valid means that the checksum values of the device image on the Junos Space server and the device match. • Invalid means that the checksum values of the device image on the Junos Space server and the device do not match. • NA means that the selected image is not staged on the device yet.
Last Checksum Time	Time when the checksum was last verified. For a device in which the selected image is not staged yet, this column displays NA .
Domain	Domain to which the device belongs

4. Select the devices on which you want to deploy the device image by using one of the following selection modes—manually, based on tags, or by using a CSV file. These options are mutually exclusive. If you select one, the others are disabled.

**TIP:**

Some points to consider when you select devices for deploying an image:

- Using a device in which the selected device image is already staged eliminates the time taken to load the device image on a device. However, if you select a device in which the image is not previously staged, then the deployment action stages the image first and then installs the image on the device. Use the **Staged** and **Not Staged** statuses on the **Staged Status** column to identify the devices in which the images are staged and not staged, respectively.

- If the **Last Checksum Time** value is way past the current time, it is better to verify the checksum before deploying the image so as to ensure that the image is valid. The deployment fails if the checksum values of the device image file on the Junos Space server and the device do not match. For more information about verifying the checksum, see [“Verifying the Checksum” on page 290](#).



NOTE: By default the **Select Device Manually** option is selected and the complete list of devices is displayed.

To select devices manually:

- Click the **Select Device Manually** option, if it is not selected previously.
- Select the devices on which you want to deploy the device image.
The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.
- To select all devices, select the check box in the column header next to Device Name.

To select devices on the basis of 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, displaying two categories of tags—Public and Private.
- 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.

To search for a specific tag, enter the first few letters of the tag name 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.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices by using a CSV file:

- Select the **Select by CSV** option.
- Click **Browse** and upload the file in .XLS format containing the list of devices on which you want to deploy the device image.



TIP: For a sample CSV file, click the [Sample CSV](#) link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

5. Select the **Show ISSU/ICU capable devices only** check box to display only those devices in which you can perform unified ISSU and ICU.
6. To specify different deployment options, select one or more of the check boxes in the **Common Deployment Options**, **Conventional Deployment Options**, **ISSU Deployment Options**, and **Advanced Options** sections.

See [Table 39 on page 298](#), [Table 40 on page 298](#), [Table 41 on page 299](#), and [Table 42 on page 300](#) for a description of the deployment options.



NOTE: When you perform a conventional upgrade of the device image on dual Routing Engines, 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.

7. (Optional) To specify common deployment options, expand the **Common Deployment Options** section and select one or more check boxes. See [Table 39 on page 298](#) for a description of the common deployment options.

Table 39: Common Deployment Options Descriptions

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 of the device image.
Delete any existing image before download	Delete all device images with the same filename from the device before deploying the selected device image.

8. (Optional) To specify conventional deployment options, expand the **Conventional Deployment Options** section and select one or more check boxes. See [Table 40 on page 298](#) for a description of the conventional deployment options.

Table 40: Conventional Deployment Options Descriptions

Conventional Deployment Options	Description
Check compatibility with current configuration	Verifies device image compatibility with the current configuration of the device

Table 40: Conventional Deployment Options Descriptions (*continued*)

Conventional Deployment Options	Description
Load succeeds if at least one statement is valid	Ensures that the device image is loaded successfully even if only one of the statements is valid
Reboot device after successful installation	Reboots 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 five 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 Series devices This check box is disabled for non-SRX Series devices.

9. (Optional) To perform unified ISSU on a dual Routing Engine device, expand the **ISSU Deployment Options** section and select one or more of the check boxes. The ISSU option is enabled only if the selected device has a dual Routing Engine. Devices with dual Routing Engines contain the **Dual RE** term in the **Platform** column of the **Select Devices** table on the Deploy Images on Devices page.

See [Table 41 on page 299](#) for a description of the unified ISSU deployment options.

Table 41: Unified ISSU Deployment Options Descriptions

Unified ISSU Deployment Options	Description
Upgrade the former Master with new image	After the backup, the 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 select this option, the former primary Routing Engine 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.

10. (Optional) To specify advanced deployment options, expand the **Advanced Options** and select one or more check boxes. See [Table 42 on page 300](#) for a description of the advanced deployment options. From this section, you can execute script bundles before and after image deployment.

Table 42: Advanced Deployment Options Descriptions

Advanced Deployment Options	Description
Execute script bundle before image deployment (pre scripts)	<p>Execute the script bundle that you have selected 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> <p>After selecting a script bundle, you can configure the script parameters of the scripts within the script bundle (for instructions, see “Step-by-Step Procedure” on page 300).</p>
Select same pre script bundle for post script bundle	<p>Execute the same script bundle on the device before and after device image deployment.</p> <p>This check box is disabled (grayed out) if you have not selected a script bundle on the Execute script bundle before image deployment (pre scripts) list.</p>
Execute script bundle after image deployment (post scripts)	<p>Execute the script bundle that you selected after deploying the device image. This ensures that the scripts in the selected script bundle is executed after the device image is installed on the device.</p> <p>After selecting a script bundle, you can configure the script parameters of the scripts within the script bundle (for instructions, see “Step-by-Step Procedure” on page 300).</p> <p>If you selected the Select same pre script bundle for post script bundle check box, then the Execute script bundle after image deployment (postscrips) check box is disabled because the postscript bundle is the same as the prescript bundle.</p>
Deploy and Enable script bundle before execution	<p>Deploy the selected script bundle, enable the scripts included in the script bundle, and then execute the script bundle on the device.</p> <p>This check box is disabled (grayed out) if you have not selected a script bundle on the Execute script bundle before image deployment (pre scripts) list or the Execute script bundle after image deployment (post scripts) list.</p>
Disable scripts after execution	<p>Execute the scripts on the script bundle on the device and then disable the scripts on the script bundle.</p> <p>You can enable the scripts at a later point of time (see “Enabling Scripts on Devices” on page 321).</p>

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 listed, you can create script bundles using the Scripts workspace (see [“Creating a Script Bundle” on page 347](#)) and then reselect the script bundle during image 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 of script parameters by clicking the icon shown below before deploying the script bundle on the 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 Devices page appears.

11. (Optional) 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 and an alert appears, displaying the job ID.



NOTE: You can monitor the progress of completion from the **Percent** column on the Job Management page.

To verify whether the image is deployed successfully, click the job ID link or navigate to the Job Management page and view the status of the job. If the job is a failure, you can double-click the job to view the reason for failure. The Device Image Action Details page displays the reason for failure in the **Description** column. However, if the image is deployed successfully, then this column displays information that is similar to the following text depending on the image and the device to which the image is deployed: **Image [12.3R1.7] to be deployed :jinstall-12.3R1.7-domestic-signed.tgz.**

Gathered Routing Engine Information.

Package installed on backup RE.

Backup RE rebooted.

Gathered software version information from backup RE.

Package installed on master RE.

Master RE rebooted.

Gathered software version information.

Also, you can export information from the Device Image Action Details page as a comma-separated values (CSV) file to your local file system.

To export data from the Device Image Action Details page to your local file system:

- a. Click **Export as CSV**.

You are prompted to save the file.

- b. Click **OK** on the File Save dialog box to save the file to your local file system.

- c. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column

to identify the devices on which the image deployment failed. See the associated Description column to understand the reasons for failure.

You can also view the result of deployment from the View Deploy Results page. See [“Viewing Device Image Deployment Results” on page 302](#).

**Related
Documentation**

- [Device Images Overview on page 273](#)
- [Uploading Device Images to Junos Space on page 285](#)
- [Script Bundles Overview on page 283](#)

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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Click the **View Deployed Results** icon.

The View Deployed Results page appears, which displays the job ID, scheduled start time, name of the image, job description, scripts executed, actual start time, end time, and the results of the device images that you deployed on devices. The columns on this page can be displayed or hidden as required.

To display or hide a column:

- a. Click the down arrow to the right of any column heading.
- b. Select **Columns**.

A list with menu options corresponding to all the available column headings appears with a check box next to each heading. The check boxes for the headings that are displayed are selected; those that are hidden are not selected.

- c. Select or deselect the headings as desired.

The tabular view changes to reflect your choices.

3. (Optional) To view only the failures in deployment, select the **Show Failures** check box. By default, this check box is unselected.

If the check box is selected, then the View Deployed Results page displays only the deployment jobs that failed.

4. (Optional) To view more information about the status of a job:

- a. On the View Deployed Results page, select a job.
- b. On the **Results** column, click the **SUCCESS** or **FAILURE** link.

The Image Deploy Results page appears, displaying the following information:

- **Image Name**—Deployed image name
- **Job Id**—Deployment job ID
- **Result**—Indicates whether the deployment is a success or failure
- **Summary**—Deployment options that you selected while deploying the image
- **Hostname**—Device to which the image is deployed
- **Comment**—More information about the status of the job

Example text, which is displayed when a deployment job is a failure:

Image [12.3R3.4] to be deployed: jinstall-ex-3300-12.3R3.4-domestic-signed.tgz
Gathered Routing Engine Information.
Failed to execute RPC request-package-add in 1024.134 seconds.
Error message from Device: null

Example text, which is displayed when a deployment job is a success:

Image [11.4R7.5] to be deployed: junos-srx1k3k-11.4R7.5-domestic.tgz
Completed copying file to the device.
Package installed on device.
Device rebooted.
Gathered software version information.

- c. (Optional) To determine whether the scripts that you chose to execute before and after image deployment were successfully executed, click the small arrow next to the hostname.

Two tables appear, which display a list of prescripts and postscripts and whether they were successfully executed.

- d. Click **Close** on the Image Deploy Results page to return to the View Deployed Results page.

5. Click the **Images** breadcrumb at the top of the View Deployed Results page to return to the Images page.

- Related Documentation**
- [Deploying Device Images on page 293](#)
 - [Staging Device Images on page 286](#)

Deleting Device Images

Using the Junos Space Network Management Platform user interface, you can delete device images from the Junos Space server as well as from devices in which they are staged.

To delete device images from the Junos Space server:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Select the images that you want to delete.

The selected images are highlighted.

3. Click the **Delete Device Images** icon.

The Delete Device Image dialog box appears and displays the image filename and the image version number. This dialog box might display a warning in scenarios where the image you are trying to delete is being staged or deployed on to devices.

4. Click **Delete** to confirm the deletion.

The selected images are deleted from Junos Space Network Management Platform and are no longer visible on the Images page.

After an image is successfully installed on a device, as an administrator, you may want to remove the staged image from the device for various reasons, such as to free space, to remove a corrupted image, and so on. You can perform this task from the Junos Space user interface on the following devices:

- BXOS
- EX Series
- JSRX Series
- M Series
- MX Series
- QF Series or QFX Series
- SSG Series
- All nodes in a cluster configuration
- Both Routing Engines in a dual Routing Engine device
- Virtual chassis

To delete device images from the devices on which they are staged:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Select the images that you want to delete.

The selected images are highlighted.

3. Select **Remove Staged Image from Device** from the Actions menu.

If the selected images are not staged on any of the devices, then Junos Space Network Management Platform displays the following error message:
None of the device(s) have all the selected image(s) staged.

If there is at least one device on which the image is staged, then the Remove Staged Image from Device page appears. This page displays the devices on which the selected images are staged. Only the devices that are common to the images selected are displayed. For example, Image1 is staged on DeviceA and DeviceB, and Image2 is staged on DeviceA. When you select Image1 and Image2 for deletion, the Remove Staged Image from Device page displays only DeviceA. This is because only DeviceA is common to both Image1 and Image2.



TIP: Before you proceed to delete an image from the devices, ensure that the Image name field displays the name of the correct image that you want to delete. If the name of a different image is displayed, click the Images breadcrumb at the top of this page to return to the Images page and select the correct image.

Use the information in [Table 43 on page 305](#) to select devices from which you want to delete the image.

Table 43: Remove Image from Staged Devices Page Information

Fields	Description
Device Image name(s)	Name of the image that you want to delete from the devices. If you select multiple images to delete, then the names of all selected images are displayed.
IP Address	IP address of the device on which the selected image is staged. You can sort the data in ascending or descending order.
Platform	Platform of the device, such as MX480, MX320, MX960, and so on. You can sort the data in ascending or descending order.
Software Version	Version of software running on the device, such as 12.3R2.5, 11.2R3.3, and so on. You can sort the data in ascending or descending order.

4. Select the devices from which you want to delete the image by using one of the following selection modes—manually, based on tags, or by using a CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the Select Device Manually option is selected and the complete list of devices is displayed.

- To select devices manually:
- a. Click the **Select Device Manually** option, if it is not selected previously.

- b. Select the devices from which you want to delete the device image.

The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

- c. To select all devices, select the check box in the column header next to Host Name.

To select devices on the basis of 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, displaying two categories of tags—Public and Private.
- c. 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.

To search for a specific tag, enter the first few letters of the tag name 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.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed. However, no devices may be listed if the image is not staged on the devices that are associated with your selected tags.

The selected tags appear 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 decrements accordingly.

To select devices using a CSV file:

- a. Select the **Select by CSV** option.
- b. Click **Browse** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.



TIP: For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application such as Microsoft Excel.

5. (Optional) Schedule the delete 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 delete operation.
 - Clear the **Schedule at a later time** check box (the default) to initiate the delete operation as soon as you click Remove.
6. Click **Remove**.

**NOTE:**

- When you delete the jinstall image, the corresponding jbundle image, if any, is also deleted from the `/var/tmp` folder on the device.
- On devices with dual Routing Engines, the image is deleted from both Routing Engines. That is, if the image is deleted from the master Routing Engine, then the image is deleted from the backup Routing Engine as well.

The image is deleted from the selected devices and an alert appears, displaying the job ID. To verify whether the image is deleted successfully, click the job ID link or navigate to the Job Management page and view the status of the job. If the job is a failure, you can double-click the job to view the reason for failure. The Job Details page appears, which displays the reason for failure in the **Description** column.

Also, you can export information from the Job Details page as a CSV file to your local file system.

To export data from the Job Details page as a CSV file to your local file system:

- a. Click **Export as CSV**.

You are prompted to save the file.

- b. Click **OK** on the File Save dialog box to save the file to your local file system.

- c. After you save the file, to return to the Job Management page, click the [X] icon on the **Exporting Device Image Job** dialog box.

When you delete a device image from a device, an audit log entry is automatically generated.

**Related
Documentation**

- [Device Images Overview on page 273](#)
- [Deploying Device Images on page 293](#)
- [Staging Device Images on page 286](#)

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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.

The Images page appears.

2. Select the image that you want to modify. The selected image is highlighted.
3. Click the **Modify Device Image** icon.

The Modify Device Image 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** field and cannot be modified.

5. To add or modify the description, you can use a maximum of 256 characters within the **Description** box.
6. 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 293](#)
- [Deleting Device Images on page 303](#)

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. If the checksum values of a device image file on the Junos Space server and the device match, then there is a high probability that the images are the same. For more information about verifying the checksum, see [“Verifying the Checksum” on page 290](#). 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 308](#)
- [Deleting the MD5 Validation Results on page 309](#)

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. On the Junos Space Network Management Platform user interface, select **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 MD5 Validation Result page displays the results of verification tasks.

[Table 44 on page 309](#) describes the Validation Results page.

Table 44: 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 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. For example, "Validation Failed."
Verification Time	Time at which you initiated verification by selecting Verify Image on Devices from the Actions menu

You can export the data from the Validation Results page as a CSV file to your local file system.

To export the data from the Validation Results page as a CSV file to your local file system:

1. Click **Export to CSV** from the Actions menu.
You are prompted to save the file.
2. Click **OK** on the File Save dialog box to save the file to your local file system.
3. After you save the file, to return to the MD5 Validation Result page, click the [X] icon on the **Exporting Validation Results** dialog box.

Navigate to the location where you saved the file and open the file by using an application such as Microsoft Excel. If you are opening this file as an Excel workbook, then filter the data for the **Failed** status in the **Checksum Result** column to identify devices on which the images are not staged completely. The **Device Image Name** column displays the images that are not staged completely.

Deleting the MD5 Validation Results

To delete the MD5 validation results:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Images**.
The Images page appears.
2. Select a device image.
3. Select **MD5 Validation Result** from the Actions menu.
The MD5 Validation Result page displays the results of all verification tasks.
4. Select the results that you want to delete.
5. Select **Delete Validation Results** from the Actions menu.

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 286](#)
 - [Verifying the Checksum on page 290](#)

CHAPTER 34

Configuration: Scripts

- [Modifying a Script on page 311](#)
- [Modifying Script Types on page 314](#)
- [Comparing Script Versions on page 314](#)
- [Deleting Scripts on page 315](#)
- [Staging Scripts on Devices on page 316](#)
- [Viewing Device Association of Scripts on page 319](#)
- [Verifying the Checksum of Scripts on Devices on page 320](#)
- [Enabling Scripts on Devices on page 321](#)
- [Disabling Scripts on Devices on page 324](#)
- [Disabling Scripts on Devices on page 326](#)
- [Removing Scripts from Devices on page 328](#)
- [Executing Scripts on Devices on page 331](#)
- [Viewing Execution Results on page 333](#)
- [Importing Scripts on page 334](#)

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 314](#).

You can modify and save the script to the Junos Space Network Management Platform database without staging the modified (or the latest) script on the devices. When you do not stage the latest version, the older script continues to exist in the devices on which it was previously staged. To combine saving and staging the modified script, use the **Save & Stage** action instead of **Save & Exit** on the Junos Space GUI.

To modify a script:

1. On the Junos Space Network Management Platform user interface, select **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 shortcut menu.

The **Modify Script** page displays the details of the script.

4. You can modify the script type, version, script contents, and the comments about the script. Script type will be disabled if it is associated to any device.

If you have multiple versions of the script, select the correct version of the script from the **Version** list to modify the script. By default, the latest version of the script is displayed. The changes that you make are saved as the latest version of the script.

5. Perform one of the following tasks:

- Click **Cancel** if you do not want to make any changes to the script.

You are returned to the Scripts page.

- Click **Save & Exit** to save the changes to the script and exit the Modify Script page. The script is saved as the latest version on the Junos Space database.

You are returned to the Scripts page.

- Click **Save & Stage** to save the changes to the script as the latest version in the Junos Space database and to stage the latest version of the script on devices.

The Stage Script on Device(s) page appears, which displays a list of all the associated devices.



TIP: If you do not see any devices listed, it means that no previous version of the script is associated with any of the devices. First, stage the script by using the **Stage Scripts on Devices** task from the Actions menu and then modify and stage the modified script by using the **Modify Script** task.

1. Select the devices on which you want the modified script to be staged, by using one of the following selection modes—manually or on the basis of tags. 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 complete list of devices is displayed. If you have tagged any of the devices and you want only those tagged devices with which the scripts are associated to be displayed, choose the **Select by tags** option.

- To select devices manually:
 - Click the **Select by Device** option and select the devices on which you want to stage the modified script. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

2. (Optional) To schedule a time for staging the script, select the **Schedule at a later time** check box and specify the date and time when you want the script to be staged.
3. Click **OK** on the Stage Script on Device(s) page.

You are returned to the Scripts page. If the modification of the script is successful, the **Latest Revision** column on this page displays the latest and updated script version number.

For troubleshooting, see the following log: `/var/log/jboss/server.log`. No audit logs are generated for this task.

To verify whether the latest script version is successfully staged on devices:

1. On the Scripts page, select the script (if it is not selected).

Typically, the script remains selected on the Scripts page when you are returned to this page after the modification of the script.

2. Select **View Associated Devices** from the Actions menu.

The View Associated Device page appears. If the staging is successful, then the version numbers on the **Latest Version** and **Staged Version** columns must match.

To return to the Scripts page, click **Scripts** on the breadcrumb.

- Related Documentation**
- [Staging Scripts on Devices on page 316](#)
 - [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. On the Junos Space Network Management Platform user interface, select **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. This action is disabled if the selected script is associated with any device.
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 value list in the **Script Type** column heading to make your changes.
5. Click **Apply**.
Your changes are saved and the 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 359](#)
 - [Staging Scripts on Devices on page 316](#)

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. On the Junos Space Network Management Platform user interface, select **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.

Next to 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 **Close** or **X** to close the window and return to the Compare Scripts page.

Related Documentation

- [Modifying a Script on page 311](#)
- [Staging Scripts on Devices on page 316](#)
- [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 with that script are deleted.

To delete scripts:

1. On the Junos Space Network Management Platform user interface, select **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 with any of the devices can be deleted. You need to remove scripts from the device before deleting the scripts from Junos Space Network Management Platform. When you delete a script, all versions of that script and the checksum verification results associated with that script are deleted.

3. Click the **Delete Scripts** icon.

You receive a confirmation message that the scripts will be deleted. If you have not removed scripts from the device before deleting the scripts from Junos Space Network Management Platform, you receive an action failure message.

The **Delete Device Scripts** dialog box lists the scripts that you chose for deletion.

4. Click **Confirm** on the Delete Device Scripts dialog box.

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 Job Management page.

If the deletion of the script fails, you can find out the reason for failure by double-clicking the row containing the job on the Job Management page. The Job Details page appears and displays the reason for failure in the **Description** column. However, if the script is deleted successfully, then the Job Details page displays the following information in this column:

Script deleted successfully

The Job Details page supports sorting of data in all columns in ascending or descending order.

5. Click **Cancel** on the Delete Device Scripts dialog box to return to the Scripts page.

Related Documentation

- [Modifying a Script on page 311](#)

Staging Scripts on Devices

Junos Space Network Management Platform enables you to stage a single script or multiple scripts on one device or multiple devices simultaneously. Staging a script enables you to hold a script on a device, ready to be executed when required. When you select scripts that are previously staged on one or more devices from the Scripts page, then the GUI lists only the devices that are not associated with any of the selected script and the devices with older versions of the selected scripts. This listing of the devices allows you

to associate scripts with new devices and also upgrade scripts to the latest version on already associated devices.

To stage a script on devices:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Scripts**.

The Scripts page appears.

2. Select the scripts that you want to stage on one or more devices. The selected scripts are highlighted.
3. Select **Stage Scripts on Devices** from the Actions menu.

The Stage Scripts on Device(s) 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 with any of the selected scripts and also the devices with the older versions of the selected scripts
4. 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.
 5. (Optional) To view the devices on which the selected scripts are staged (or with which the selected scripts are associated), select the **Show existing Staged Devices** check box. Typically, Junos Space Network Management Platform displays a list of devices that are not associated with any of the selected scripts.
 6. Select the devices to stage the selected script.

You can select devices by using one of the following selection modes—manually, on the basis of tags, or by using a CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- To select devices manually:
 - Click the **Select by Device** option and select the devices on which you want to stage the script. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
 - To select all devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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 the devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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 on the Select Devices status bar decrements accordingly.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option on the Stage Scripts on Device(s) page.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

7. (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.
8. Click **Stage**. The script is staged on the selected device or devices. The Stage Scripts Information dialog box displays the job ID.
9. Perform one of the following actions on the Stage Scripts Information dialog box:
 - To verify the status of this job, click the job ID on this dialog box.
 - Click **OK** to go back to the Scripts page.

On the Scripts page, click **View** in the **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 version, 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 319](#).

If there is a failure in the staging of the script, you can view the reason for failure within the job description on the Job Management page.

You can export details about staging of a script as a comma-separated values (CSV) file to your local file system:

1. Double-click the job pertaining to the staging operation.
The Script Management Job Status page appears.
2. Click **Export as CSV**.
You are prompted to save the file.
3. Click **OK** on the File Save dialog box to save the file to your local file system.
4. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** dialog box.
Use an application such as Microsoft Excel to open the downloaded file from your local system.

- Related Documentation**
- [Scripts Overview on page 275](#)
 - [Viewing Device Association of Scripts on page 319](#)

Viewing Device Association of Scripts

You can view the details of multiple scripts that are 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 **View** in the **Associations** column on the Scripts page displays the associated devices for a single script.

To view devices that are associated with scripts:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Scripts**.
The Scripts page appears.
2. Select a script.



NOTE: Make sure that the script is previously staged to the devices using Junos Space Network Management Platform.

3. Select **View Associated Devices** from the Actions menu.

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, domain, and activation status.

4. Click **Back** to go back to the **Scripts** page.

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

- [Staging Scripts on Devices on page 316](#)

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 the 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 receive an error message.

To verify the checksum of a script:

1. On the Junos Space Network Management Platform user interface, select **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. From the Actions menu, 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 one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- To select devices manually:
 - Click the **Select by Device** option and select the devices that have the script deployed on them. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

5. 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.
6. Click **Verify Checksum**.

The result of this verification appears, and a **Jobs** dialog box displays a job ID link.

Perform one of the following actions on the jobs dialog box:

- Click the job ID link to view the status of the verification operation on the Jobs page.
- Click **Cancel** on the jobs dialog box to return to the Scripts page.

To display the checksum verification results, see [“Viewing Verification Results” on page 360](#).

Related Documentation

- [Enabling Scripts on Devices on page 321](#)

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. On the Junos Space Network Management Platform user interface, select **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. If the selected scripts are already enabled on the devices, then Junos Space displays the following message instead of the Enable Scripts on Device(s) page:

Device(s) having all the selected staged script(s) already have them in enabled state.



NOTE:

- This operation does not list devices that are not associated with scripts. It also does not list the devices for which the script is in an enabled state already.
 - If you select multiple scripts, then devices that are commonly associated with all the selected scripts are only displayed.
-

4. Select the devices on which you want the script to be enabled, by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- To select devices manually:
 - Click the **Select by Device** option and select the devices on which you want to enable the device script. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

5. (Optional) 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.
6. Click **Enable**.

The selected scripts are enabled on the devices, and the Enable Scripts Information dialog box displays a link to the job ID.

Perform one of the following actions on the Enable Scripts Information dialog box

- Click the job ID link to view the status of this task on the Job Management page.
- Click **OK** to return to the Scripts page.

You can export details about enabling of a script as a comma-separated values (CSV) file to your local file system:

1. Double-click the job pertaining to the script enabling operation.

The Script Management Job Status page appears.

2. Click **Export as CSV**.

You are prompted to save the file.

3. Click **OK** on the File Save dialog box to save the file to your local file system.

4. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system.

**Related
Documentation**

- [Executing Scripts on Devices on page 331](#)

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 using 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. On the Junos Space Network Management Platform user interface, select **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. If the selected scripts are already disabled on the devices, then Junos Space displays the following message instead of the Disable Scripts on Device(s) page:

Device(s) having all the selected staged script(s) already have them in disabled state.

4. Select the devices on which you want the script to be disabled, by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete 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; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
6. To select devices on the basis of 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, displaying two categories of tags—Public and Private. A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

7. To select devices by using a CSV file:

- Select the **Select by CSV** option.
- Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

8. 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.

9. Click **Disable**.

The selected scripts are disabled on the devices, and the Disable Scripts Information dialog box displays a link to the job ID. You can click the link to view the status of this task on the Job Management page.

To return to the Scripts page, click **Scripts** on the left pane.

Related Documentation

- [Scripts Overview on page 275](#)

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 using 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. On the Junos Space Network Management Platform user interface, select **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. If the selected scripts are already disabled on the devices, then Junos Space displays the following message instead of the Disable Scripts on Device(s) page:

Device(s) having all the selected staged script(s) already have them in disabled state.

4. Select the devices on which you want the script to be disabled, by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete 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; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.

6. To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

7. To select devices by using a CSV file:

- Select the **Select by CSV** option.
- Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

8. 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.
9. Click **Disable**.

The selected scripts are disabled on the devices, and the Disable Scripts Information dialog box displays a link to the job ID. You can click the link to view the status of this task on the Job Management page.

To return to the Scripts page, click **Scripts** on the left pane.

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 with the selected scripts. If you select multiple scripts, then the devices that are associated with all the scripts are only displayed on the Remove Scripts from Device(s) page.



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. On the Junos Space Network Management Platform user interface, select **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) dialog box appears and it displays the devices the script is associated with.

4. Select the devices from which you want the script to be removed, by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed. For multiple selection, only commonly associated devices are listed.

- 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; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

5. Select the **Force Remove** check box to remove the script-device association from Junos Space Network Management Platform even if it is unable to remove the scripts from the devices due to connectivity issues. You need to turn this option on before you remove the scripts. The script-device association is removed regardless of whether this operation has failed or not.

6. Click **Remove**.

The script is removed from the selected devices, and the Remove Scripts Information dialog box appears, which displays a job ID link. You can click the link to view the status of the script removal operation on the Job Management page.

Perform one of the following actions on the Remove Scripts Information dialog box:

- Click the job ID link to view the status of the script removal operation on the Job Management page.
- Click **OK** to return to the Scripts page.

On the **Scripts** page, click **View** listed in 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 are removed.

If the removal of the script fails, you can find out the reason for failure by double-clicking the row containing the job on the Job Management page. The Job Details page appears and displays the reason for failure in the **Description** column. However, if the script is removed successfully, then the Job Details page displays the following information in this column:

Script removed successfully from the devices

The Job Details page supports sorting of data in all columns in ascending or descending order.

You can export details about the removal of a script as a comma-separated values (CSV) file to your local file system:

1. Double-click the job pertaining to the removal of scripts.

The Script Management Job Status page appears.

2. Click **Export as CSV**.

You are prompted to save the file.

3. Click **OK** on the File Save dialog box to save the file to your local file system.

4. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system.

- Related Documentation**
- [Staging Scripts on Devices on page 316](#)
 - [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 are triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or at a specific time, 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. On the Junos Space Network Management Platform user interface, select **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 Devices** 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. If the selected script is already disabled on the devices, then Junos Space displays the following message instead of the Execute Scripts on Device(s) page:

Disabled script cannot be executed.

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.



NOTE: A quick way to find out which version of the script is staged, click **View** in the **Associations** column on 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 one of the following selection modes—manually, on the basis of tags, or by using a CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- 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; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

5. (Optional) To specify values for the parameters for script execution, click **Enter Parameter Value** for each parameter.
6. (Optional) 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.
7. Click **Execute**.

The selected scripts are executed on the devices, and the Execute Script Information dialog box displays a link to the job ID. You can click the link to view the status of this task on the Job Management page. Double-click the task to view the Script

Management Job status page. Click the **View Results** link in the **Description** column to view the results of script execution. The Script Execution Job Results page allows you to read and understand the Script Execution Results. Click the X icon to close this page.

You can export details about the execution of a script as a comma-separated values (CSV) file to your local file system:

1. Double-click the job pertaining to the script execution operation.

The Script Management Job Status page appears.

2. Click **Export as CSV**.

You are prompted to save the file.

3. Click **OK** on the File Save dialog box to save the file to your local file system.

4. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. Typically, you can view the script output on the Description column on this file.

To return to the Scripts page, click **Scripts** on the left pane.

You can view the script execution from the Device Management page (Devices > Device Management) by selecting one or more devices and selecting **View Script Executions** from the shortcut menu (Devices > Device Management > Select a device > Device Inventory). 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 321](#)
- [Executing Scripts on Devices Locally with JUISE on page 78](#)

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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Scripts**.

The **Scripts** page appears.

2. Click the **View Execution Results** icon.

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 45 on page 334](#) describes the information that appears on the View Execution Results page.

Table 45: View Execution Results 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 of the script started
Execution End Time	The time at which the execution of the script ended

3. Click the **View** link under the **Results** column to view the detailed execution results.

The Script Execution Job Results dialog box appears and displays the results of the script execution.

- Related Documentation**
- [Executing Scripts on Devices on page 331](#)
 - [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 **Import Script** icon. 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
- Modify script
- Delete scripts
- Enable and disable scripts on devices

- Execute script on devices
- View execution results
- Remove scripts from devices
- Stage scripts on devices
- Compare scripts versions
- Export scripts
- Modify scripts type
- View associated devices
- View verification results
- Verify the checksum of scripts
- Tag and untag scripts, view the scripts that are tagged, delete private tags

Prior to Junos 9.0, event scripts and op scripts were saved in op directory and enabled under system scripts op hierarchy. However, beginning from 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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Scripts** .
The Scripts page appears.
2. Click the **Import Script** icon.
The Import Script page appears.
3. On the Import Script page, click the Add Device Scripts icon. The Add Device Scripts page appears.
4. Click **Browse**. The file upload dialog box displays the directories and folders on your local file system.
5. Select the script or scripts that you want to import (you can select a maximum of 680 scripts at a time), and click **Open**.
6. Click **Add Script(s)** to upload the scripts, or click **Cancel** if you want to go back to the **Import Script** page.



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 Network Management Platform using the Log Out button, the temporary session folders are deleted after 30 minutes.

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.

7. If you want to remove any scripts that are displayed in the Import Script page, select the scripts and click the **Delete Scripts** icon.
8. Click **Import Scripts**. The selected scripts are uploaded into Junos Space Network Management Platform and are displayed on the Scripts page.

If the script files already exist on Junos Space Network Management Platform, then it displays the following message. Click **Yes** or **No** as required.

Some device script file already exists. Do you want to replace all versions of the existing script file? List of existing script file(s): * op-fpc-restart.slax * op-re-status.slax * op-re-switch.slax

9. To return to the Scripts page, click **Scripts** on the left panes.

Related Documentation

- [Viewing Script Details on page 359](#)

Configuration: Operations

- [Creating an Operation on page 337](#)
- [Modifying an Operation on page 340](#)
- [Running an Operation on page 341](#)
- [Copying an Operation on page 342](#)
- [Deleting an Operation on page 343](#)
- [Exporting an Operation in .tar Format on page 344](#)
- [Importing an Operation on page 345](#)

Creating an Operation

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade to 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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Operations**.

The Operations page appears.

2. Click the Create Operation icon.

The Create Operation page appears.

3. In the **Name** text box, type a user-defined script bundle name.

The operation name cannot exceed 32 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.). The name cannot start with a space.

4. In the **Description** text box, type a user-defined script bundle description.

The operation description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Select the **Mark as important** check box to mark this operation as important.
6. 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** page appears. This page displays all the available scripts on the Junos Space Network Management Platform. To search for a specific script, you can enter the search criteria on the Search field on top right of this page. To clear the search results, click the x icon next to the search criteria.

Select the scripts and click **Add** to add your selections to the list. You are returned to the Create Operation page.

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 Script** 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—If you have opted to execute the script, then you can configure the script return code, which provides you with the information about whether the script execution was a success or a failure. Junos Space Network Management Platform, 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:

In the **Set Return Code** section:

- 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 Device Image** page appears. This page displays all the available images on the Junos Space Network Management Platform. To search for a specific image, you can enter the search criteria on the Search field on top right of this page. To clear the search results, click the x icon next to the search criteria.

Select the images and click **Add** to add your selections to the list.

You can also edit the action that image should perform (for example, **Stage** or **Deploy**), and various other deployment options. See [“Deploying Device Images” on page 293](#) for more information.

- To add an operation, click the Add (+) icon, and select **Operation** from the list. The **Select Operations** page appears. This page displays all the available operations on the Junos Space Network Management Platform. To search for a specific operation, you can enter the search criteria on the Search field on the top right of this page. To clear the search results, click the X icon next to the search criteria.

Select the operations and click **Add** to add your selections to the list.



NOTE: You cannot edit a child operation.

7. You can modify the list of selected scripts, images, and operations using the icons described in [Table 46 on page 339](#).

Table 46: 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.
	<p>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 293 for more information.</p> <p>NOTE: You cannot edit a child operation.</p>

8. Click **Create** to create the operation.

You are returned to the Operations page. If the operation is successfully created, then you can view the newly added operation on this page. An operation that is marked important appears with a star next to it indicating that this operation takes priority over others (the star appears in the **Priority** column on 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 281](#)
- [Modifying an Operation on page 340](#)
- [Running an Operation on page 341](#)
- [Copying an Operation on page 342](#)
- [Viewing Operations Results on page 363](#)
- [Deleting an Operation on page 343](#)
- [Exporting an Operation in .tar Format on page 344](#)
- [Importing an Operation on page 345](#)

Modifying an Operation

Junos Space Network Management Platform allows you to edit the parameters of an operation.

To modify an operation:

1. On the Junos Space Network Management Platform user interface, 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 337](#) 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 281](#)
- [Creating an Operation on page 337](#)
- [Running an Operation on page 341](#)
- [Copying an Operation on page 342](#)

- [Viewing Operations Results on page 363](#)
- [Deleting an Operation on page 343](#)
- [Exporting an Operation in .tar Format on page 344](#)
- [Importing an Operation on page 345](#)

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. On the Junos Space Network Management Platform user interface, 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 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 Search field at the top of the Run Operation page.

5. (Optional) You can also specify a tag for the selected devices on the **Tag Selected Devices As** field so that you can reuse the same group of devices to run a different operation.
6. (Optional) You can also schedule a time for the operation to run by selecting the **Schedule at a later time** check box and specifying the date and time when you want to run the operation.
7. Click **OK**. The selected operation is executed on the devices, and the Operation Execution Information dialog box displays a link to the job. Perform one of the following actions on the jobs dialog box:
 - Click the job ID link to view the status of the operation execution on the Job Management page. If the execution of the operation fails, you can find out the reason for failure by double-clicking this job on the Job Management page. The job details page appears. Double click the row displaying failure in the **Result** column. The scripts, image, and operations that failed are listed. Click the **Failure** link to know the reason for failure.

You can sort the displayed data in ascending or descending order.

- Click **OK** to return to the Operations page.

You can export details about the execution of an operation as a comma-separated values (CSV) file to your local system:

- a. On the Job Management page, double-click the job pertaining to this operation.

The Operation Result Detail page appears.

- b. Click **Export as CSV**.

You are prompted to save the file.

- c. Click **OK** on the File Save dialog box to save the file to your local file system.

- d. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Operation Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system.

Related Documentation

- [Operations Overview on page 281](#)
- [Creating an Operation on page 337](#)
- [Modifying an Operation on page 340](#)
- [Copying an Operation on page 342](#)
- [Viewing Operations Results on page 363](#)
- [Deleting an Operation on page 343](#)
- [Exporting an Operation in .tar Format on page 344](#)
- [Importing an Operation on page 345](#)

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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Operations**.

The **Operations** page displays the operations in Junos Space Network Management Platform.

2. Select the operation that you want to copy.
3. Select **Clone Operation** from the shortcut 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** field.
5. Click **Copy** to create a copy of the operation and go back to the Operations page.

- Related Documentation**
- [Operations Overview on page 281](#)
 - [Creating an Operation on page 337](#)
 - [Modifying an Operation on page 340](#)
 - [Running an Operation on page 341](#)
 - [Deleting an Operation on page 343](#)
 - [Viewing Operations Results on page 363](#)

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. On the Junos Space Network Management Platform user interface, select **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 shortcut menu.

The **Delete Operations** dialog box lists the operations that you chose for deletion.

4. Click **Delete** to delete the operation.

The selected operations are deleted.



NOTE: When you delete an operation, you do not delete the scripts, images or operations associated with this operation from the Junos Space Network Management Platform database.

- Related Documentation**
- [Operations Overview on page 281](#)
 - [Creating an Operation on page 337](#)
 - [Modifying an Operation on page 340](#)
 - [Running an Operation on page 341](#)
 - [Copying an Operation on page 342](#)
 - [Viewing Operations Results on page 363](#)

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. On the Junos Space Network Management Platform user interface, 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** on the Export Operations page.

The File Open dialog box appears and enables you to save the operation files in .tar format and the **Export Operations Job Status** dialog box displays the status of this task. To view the status of your job, click the bar on the Export Operations Job Status dialog box.

5. Click **OK** in the File Open dialog box to save the files to your local file system. Alternatively, you can save the .tar file by clicking the **Download** link in the Export Operations Job Status dialog box.
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 281](#)
 - [Creating an Operation on page 337](#)
 - [Modifying an Operation on page 340](#)
 - [Running an Operation on page 341](#)
 - [Copying an Operation on page 342](#)
 - [Viewing Operations Results on page 363](#)
 - [Deleting an Operation on page 343](#)
 - [Importing an Operation on page 345](#)

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:

- The files are in .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. For more information about creating and exporting an operation, see [“Creating an Operation” on page 337](#) and [“Exporting an Operation in .tar Format” on page 344](#).



NOTE: If you want to import multiple operations at a time, use the Mozilla Firefox or Google 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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Operations**.

The Operations page appears.

2. Click 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 Mozilla Firefox or Google Chrome to import multiple operations. Currently, using Internet Explorer, you can import only a 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 281](#)
- [Creating an Operation on page 337](#)
- [Modifying an Operation on page 340](#)
- [Running an Operation on page 341](#)
- [Copying an Operation on page 342](#)
- [Viewing Operations Results on page 363](#)
- [Deleting an Operation on page 343](#)
- [Exporting an Operation in .tar Format on page 344](#)

Configuration: Script Bundles

- [Creating a Script Bundle on page 347](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Staging Script Bundles on Devices on page 350](#)
- [Executing Script Bundles on Devices on page 353](#)
- [Enabling Scripts in Script Bundles on Devices on page 355](#)
- [Disabling Scripts in Script Bundles on Devices on page 356](#)

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 334](#)).

To create a script bundle:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Script Bundles** and select the **Create Script Bundle** icon.


The Create Script Bundle page appears.

2. In the **Name** text box, type a user-defined operation name.

The script bundle name cannot exceed 50 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.). The name cannot start with a space.

3. In the **Description** text box, type a user-defined operation description.

The script bundle description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

4. 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.

5. Select the scripts that you want to include in the script bundle.
The selected scripts are highlighted.







6. Click **Add**.

The selected scripts are included in the **Selected Scripts** section of the **Create Script Bundle** page.

7. On the Create Script Bundle page, under the Selected Scripts section, you can edit the script parameters, rule, and version.
 - To change the version of the script, click the Edit icon next to **selected Version** for the script and select the suitable version from the drop-down list. By default, the latest version of the script is associated with the script bundle.
 - You can set success or failure criteria based on the script output. When you set criteria, the script execution is considered a success or a failure only if the specified criteria (text string) is present in the execution results. By default, no specific strings are searched in the script output and if the script is executed without any errors, then the execution is considered to be a success.
 - After selection, click **Save**.

On this page, you can also modify the list of selected scripts using the icons described in [Table 47 on page 348](#).

Table 47: 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 or the script version. This option is disabled when commit scripts are selected.

8. 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 350](#)

- [Modifying a Script Bundle on page 349](#)
- [Scripts Overview on page 275](#)

Modifying a Script Bundle

Junos Space Network Management Platform allows you to modify a script bundle's 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:

1. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Script Bundles**.

The Script Bundles page displays all Junos Space Network Management Platform script bundles.

2. Select the script bundle that you want to modify.
3. Click the **Modify Script Bundle** icon.
The **Modify Script Bundle** page appears.
4. Make your changes to the 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 48 on page 349](#).

Table 48: 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.

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 350](#)
 - [Executing Script Bundles on Devices on page 353](#)
 - [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. On the Junos Space Network Management Platform user interface, 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 appears and displays the names of the selected script bundles.
4. Click **Delete** to confirm that you want to delete the selected script bundles.
Jobs dialog box appears displaying a job ID link. Perform one of the following actions on the jobs dialog box:
 - Click the job ID link to view the status of the delete operation on the Job Management page. If the deletion of the script bundles fail, you can find out the reason for failure by double-clicking this job on the Job Management page. The job details page appears and displays the reason for failure in the Description column. The job details page supports sorting of data in all columns in ascending or descending order.
 - Click **OK** to return to the Scripts Bundles page.

If the script bundles are successfully deleted, then the deleted script bundles are not listed on the Script Bundles page.

- Related Documentation**
- [Creating a Script Bundle on page 347](#)
 - [Executing Script Bundles on Devices on page 353](#)
 - [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 the FPCs.

To stage script bundles on devices:

1. On the Junos Space Network Management Platform user interface, 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 stage on devices.
3. Select **Stage Script Bundle on Devices** from the Actions menu.
The **Stage Script Bundle On Device(s)** dialog box appears.
4. Keep the **Enable Scripts on Devices** 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.

5. 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.
6. Select the devices on which you want to stage the script bundles.

You can select devices by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- To select devices manually:
 - Click the **Select by Device** option and select the devices on which you want to enable the device script. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

7. (Optional) 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.

8. Click **Stage**.

The selected scripts are deployed and a jobs dialog box appears displaying a job ID link. Perform one of the following actions on the jobs dialog box:

- Click the job ID link to view the status of the staging operation on the Job Management page. If the staging of the script bundles fail, you can find out the reason for failure by double-clicking this job on the Job Management page. The job details page appears and displays the reason for failure in the Description column. The job details page supports sorting of data in all columns in ascending or descending order.
- Click **OK** to return to the Scripts Bundles page.

Related Documentation

- [Creating a Script Bundle on page 347](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Executing Script Bundles on Devices on page 353](#)
- [Enabling Scripts in Script Bundles on Devices on page 355](#)
- [Disabling Scripts in Script Bundles on Devices on page 356](#)
- [Script Bundles Overview on page 283](#)

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. On the Junos Space Network Management Platform user interface, 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 execute on devices.
3. Right-click your selection or use the Actions menu, and select **Execute Script Bundle 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.

You can select devices by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.



NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

- To select devices manually:
 - Click the **Select by Device** option and select the devices on which you want to enable the device script. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
 - To select all the devices, select the check box in the column header next to Host Name.
- To select devices on the basis of 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, displaying two categories of tags—Public and Private.

A check box is displayed next to each tag name, which you can select to select a specific tag.

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.

The table below this status bar displays the selected devices.

- To select devices by using a CSV file:
 - Select the **Select by CSV** option.
 - Click **Select by CSV** and upload the file in .xls format containing the list of devices on which you want to deploy the device image.

For a sample CSV file, click the **Sample CSV** link.

5. (Optional) 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. On the Execute Script Bundle On Device(s) page, click the **Update Script Parameters/Rule** link. The **Configure Script Bundle Parameters** dialog box appears.
2. Click **set value** to edit the script parameters and click **Save**.

You can also set success or failure criteria based on the script output. When you set criteria, the script execution is considered a success or a failure only if the specified criteria (text string) is present in the execution results. By default, no specific strings are searched in the script output and if the script is executed without any errors, then the execution is considered to be a success.

3. Click **Configure**. Your changes are saved and the **Enable Script Bundle On Device(s)** dialog box displays your previous selections.

6. (Optional) 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 and executed on the selected devices and a jobs dialog box displays a job ID link. Perform one of the following actions on the jobs dialog box:
 - Click the job ID link to view the status of execution on the Job Management page. If the execution of the script bundles fail, you can find out the reason for failure by double-clicking this job on the Job Management page. The job details page appears and displays the reason for failure in the Description column. The job details page supports sorting of data in all columns in ascending or descending order.
 - Click **OK** to return to the Scripts Bundles page.

Related Documentation

- [Creating a Script Bundle on page 347](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Staging Script Bundles on Devices on page 350](#)
- [Enabling Scripts in Script Bundles on Devices on page 355](#)
- [Disabling Scripts in Script Bundles on Devices on page 356](#)
- [Script Bundles Overview on page 283](#)

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. On the Junos Space Network Management Platform user interface, 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 with 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 a jobs dialog box displays a job ID link. Perform one of the following actions on the jobs dialog box:

- Click the job ID link to view the job status on the Job Management page. If the scripts are not enabled on the selected devices, you can find out the reason for failure by double-clicking this job on the Job Management page. The job details page appears and displays the reason for failure in the Description column. The job details page supports sorting of data in all columns in ascending or descending order.
- Click **OK** to return to the Scripts Bundles page.

**Related
Documentation**

- [Disabling Scripts in Script Bundles on Devices on page 356](#)
- [Creating a Script Bundle on page 347](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Staging Script Bundles on Devices on page 350](#)
- [Executing Script Bundles on Devices on page 353](#)
- [Script Bundles Overview on page 283](#)

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. On Junos Space Network Management Platform, 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. Perform one of the following actions on the jobs dialog box:

- Click the job ID link to view the job status on the Job Management page. If the scripts are not disabled on the selected devices, you can find out the reason for failure by double-clicking this job on the Job Management page. The job details page appears and displays the reason for failure in the Description column. The job details page supports sorting of data in all columns in ascending or descending order.
- Click **OK** to return to the Scripts Bundles page.

Related Documentation

- [Enabling Scripts in Script Bundles on Devices on page 355](#)

- [Viewing Device Associations of Scripts in Script Bundles on page 365](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Staging Script Bundles on Devices on page 350](#)
- [Executing Script Bundles on Devices on page 353](#)
- [Script Bundles Overview on page 283](#)

Administration: Scripts

- [Viewing Script Details on page 359](#)
- [Viewing Verification Results on page 360](#)
- [Exporting Scripts in .tar Format on page 361](#)
- [Scripts User Roles on page 362](#)

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. On the Junos Space Network Management Platform user interface, select **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** page displays the script name, type, format, creation time, version, script contents, and comments. Use the scroll bar to the right of this page to scroll through the script.

[Table 49 on page 359](#) describes the fields displayed on the Script Details page.

Table 49: Script Details Dialog Box Fields

Field	Description
Name	Name of the script file
Type	Type of script. The values can be one of the following: <ul style="list-style-type: none">• Commit script• Op script• Event script

Table 49: Script Details Dialog Box Fields (*continued*)

Field	Description
Format	Format of the script file. The values can be one of the following: <ul style="list-style-type: none"> • XSL • SLAX
Creation Time	Date and time when the script was created
Version	Version number of the script. When you modify a script, the changes are saved as the latest version of the script.
Script contents	Contents of the script
Comments	Text that describes the script that is entered by the user
Related Documentation	<ul style="list-style-type: none"> • Scripts Overview on page 275 • Exporting Scripts in .tar Format on page 361

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 with that script are also deleted.

Verifying the checksum of the scripts that use Junos Space Network Management Platform ensures that the script transferred to a device is not corrupt. For more information about verifying the checksum of a script, see [“Verifying the Checksum of Scripts on Devices” on page 320](#).

To view the verification results:

1. On the Junos Space Network Management Platform user interface, select **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 results you want to view.
3. Right-click your selection or use the Actions menu, and select **Verification Results**.

The **Script Verification Results** page displays the results of the checksum verification.

[Table 50 on page 361](#) describes the fields on the Script Verification Results page.

Table 50: 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 could be one of the following: <ul style="list-style-type: none"> • Success • Failed
Comments	

4. Click **Back** to return to the Scripts page.

Related Documentation

- [Executing Scripts on Devices on page 331](#)

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 in .tar format:

1. On the Junos Space Network Management Platform user interface, select **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 export.
3. Select **Export Scripts** from the Actions menu.
The **Export Scripts** dialog box asks you for confirmation.
4. Click **Export**.
The **File Open** dialog box enables you to save the script files in .tar format and the **Export Scripts Job Status** dialog box displays the status of this task graphically.
5. Click **OK** in the File Open dialog box to save the files to your local file system.
Alternatively, you can save the .tar file by clicking the **Download** link in the Export Operations Job Status dialog box.
6. Perform one of the following actions on the Export Scripts Job Status dialog box:
 - To view the status of your job on the Job Management page, click the bar on this dialog box.
 - To return to the Scripts page, click the X icon on this dialog box.

Navigate to the folder in your local file system and unzip the files to view the contents of the script.

Related Documentation

- [Scripts Overview on page 275](#)

Scripts 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 each user you can access and perform different tasks. You cannot view the pages to which you do not have access to. You can create users and manage them on the Users page. If you have User Administrator permissions to create and manage users, navigate to Network Management Platform > Role Base Access control > User Accounts. The User Accounts page lists the existing users. Use this page to create and assign roles to the Scripts users.

You can enable and disable scripts on devices using Junos Space Network Management Platform only if you are a super user with complete permissions or a user who has been given maintenance privileges.



NOTE: The Junos OS management process executes commit scripts with root permissions, and 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.

The Scripts tasks that different users have access to, based on the roles assigned to them is listed in [Table 51 on page 362](#).

Table 51: Scripts User Roles

User Role	Permitted Tasks
Device Script Manager	Viewing, importing, modifying, comparing, deleting, deploying, enabling, disabling, verifying, removing, executing scripts and viewing results
Device Script Read Only User	View execution results, view associated devices, compare, export scripts
Device Script Operator	Executing scripts and viewing execution results.

Related Documentation

- [Scripts Overview on page 275](#)
- [Script Example on page 371](#)

Administration: Operations

- [Viewing Operations Results on page 363](#)

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. On the Junos Space Network Management Platform user interface, select **Images and Scripts > Operations**.

The Operations page appears.

2. Click the **View Operation Results** icon.

The View Operation Results page appears and displays the following information:

- 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

Most parameters on the View Operation Results page have the drop down list enabled with the filter option, wherein you can specify the filter criteria. On applying the filters, the table contents display only the values that match the filter criteria.

3. (Optional) Double-click an operation to open the **Operation Result Detail** page, 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).

4. (Optional) On the Operation Result Detail page, click a row to view the success or failure details.
5. (Optional) On the Operation Result Detail page, click **Export as CSV** to export the operation results. The Export as CSV page appears displaying the results in .csv format.

To exit this page, click the **X** symbol at the top-right corner of this page. You are returned to the Operation Result Detail page.

6. Click **Close** on the Operation Result Detail page to go back to the View Operation Results page.

**Related
Documentation**

- [Operations Overview on page 281](#)
- [Creating an Operation on page 337](#)
- [Modifying an Operation on page 340](#)
- [Running an Operation on page 341](#)
- [Copying an Operation on page 342](#)
- [Deleting an Operation on page 343](#)

Administration: Script Bundles

- [Viewing Device Associations of Scripts in Script Bundles on page 365](#)

Viewing Device Associations of 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. On the Junos Space Network Management Platform user interface, 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) with 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 the domain to which they belong to.

4. Click **Back** to go back to the Script Bundles page.

Related Documentation

- [Enabling Scripts in Script Bundles on Devices on page 355](#)
- [Disabling Scripts in Script Bundles on Devices on page 356](#)
- [Modifying a Script Bundle on page 349](#)
- [Deleting Script Bundles on page 350](#)
- [Staging Script Bundles on Devices on page 350](#)
- [Executing Script Bundles on Devices on page 353](#)
- [Script Bundles Overview on page 283](#)

Annotations and Examples

- [Scripts Annotations on page 367](#)
- [Script Example on page 371](#)

Scripts Annotations

Script annotations are used to specify the metadata of a script. They are embedded as a part of scripts. They are parsed and stored in space DB while importing or modifying scripts. An annotation is specified using the following syntax.

```
/* @[ANNOTATION]= "<ANNOTATION CONTENT>" */
```

The annotation can be provided anywhere in the script.

Annotations are used to provide the script context, name , description, and confirmation text. For an example script with the annotation, see ["Script Example" on page 371](#).

Annotation	Description
@CONTEXT	<p>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. Example:</p> <pre>/* @CONTEXT = "/device/chassis-inventory/chassis/chassis-module[starts-with(name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]" */</pre>
@NAME	<p>Used to give the descriptive name of the script. Example:</p> <pre>/* @NAME = "Put PIC Offline" */</pre>
@DESCRIPTION	<p>Used to give the description of the script. Example:</p> <pre>/* @DESCRIPTION = "Take PIC offline." */</pre>

Annotation	Description
@CONFIRMATION	<p>Used to give the confirmation text of the script, that is, 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.</p> <p>Example:</p> <pre>/* @CONFIRMATION = "Are you sure that you want to take the PIC offline?" */</pre>
@EXECUTIONTYPE	<p>The type of execution are GROUPEDEXECUTION and SINGLEEXECUTION. When this annotation is not specified, the default option would be SINGLEEXECUTION.</p> <p>Example:</p> <pre>/* @EXECUTIONTYPE = "SINGLEEXECUTION" */</pre>
@ISLOCAL	<p>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</p> <p>Example:</p> <pre>/*@ISLOCAL="true"*/</pre>
@VARIABLECONTEXT	<p>Used to define the context of a variable.</p> <p>Example:</p> <pre>/*@VARIABLECONTEXT="[{ 'name': 'XPATHVARIABLE1', 'defaultvalue': 'mydefaultvalue', 'parameterscope': 'devicespecific' }, { 'name': 'XPATHVARIABLE2', 'configuredvaluexpath': '/device/interface-information/physical-interface/name/text()', 'parameterscope': 'entityspecific' }, { 'name': 'XPATHVARIABLE3', 'selectionvaluesxpath': '/device/interface-information/physical-interface/name/text()', 'parameterscope': 'global' }]"*/</pre>
@PASSSPACEAUTHHEADER	<p>This annotation is specific to local scripts, if the value of this annotation is to true, then the script variables \$JSESSIONSSO and \$JSESSIONID would be set.</p> <p>Example:</p> <pre>/*@PASSSPACEAUTHHEADER="true"*/</pre> <p>Also provides the virtual IP of the cluster in \$VIP.</p>
@PASSDEVICECREDENTIALS	<p>This annotation is specific to local scripts. If this annotation is set to true, Junos Space Network Management Platform sets the device credentials to the variable \$credentials and \$deviceipmap (i.e. \$deviceipmap= '{ "192.168.0.210": "Device1", ... }')..</p> <p>Example:</p> <pre>/*@ PASSDEVICECREDENTIALS = "true"*/</pre>
@PROMOTE	<p>This annotation is used to define whether the script is available for execution as a right click action. This only works for @EXECUTIONTYPE = "SINGLEEXECUTION"</p>

Annotation	Description
@ONCLOSESTRING	This annotation is used when the user wants the script execution result screen to be closed automatically once the expected result is received. The @ONCLOSESTRING annotation contains a string. This string is compared with the script execution results. When the specified string appears in the script output, the script execution result is automatically closed. The @ONCLOSESTRING annotation is useful in case of script promotion. For example – The user has included @ONCLOSESTRING annotation in the Reboot script containing a string that is displayed on successful execution of script. If the user executes that promoted Reboot script the result window closes by itself the reboot command has been sent to the device successfully. Otherwise it displays the reason for failure in result window. This further improves the user experience by reducing the number of clicks required by the user in order to complete an action.

Script Execution Types

When the script execution type is SINGLEEXECUTION, the script cannot be executed for multiple elements. This can be helpful if the script developer wants to ensure that script execution should not be triggered for multiple elements at once.

When GROUPEDEXECUTION is specified as the 'Script execution type' and multiple elements are selected for execution, the script is run only once for all the selected elements. If multiple devices are selected, then one execution happens per device. The elements are grouped based on the devices and execution happens once for each group. The context of elements belonging to the group is passed as an expression to the \$CONTEXT variable in the script. This way, the script is provided with the elements the script should be executed for.

For example for GROUPEDEXECUTION the context structure could be defined as:

```
/device[name="EX4200-20"]/interface-information/physical-interface[name="ge-0/0/11"]
/device[name="EX4200-20"]/interface-information/physical-interface[name="ge-0/0/12"],
/device[name="EX4200-240"]/interface-information/physical-interface[name="ge-0/0/5"]
/device[name="EX4200-240"]/interface-information/physical-interface[name="ge-0/0/6"].
```

Variable Context

Context of a variable defines what input the script is expecting from the user. This context can be used to auto-populate user input options. This behavior is similar to parameters in configlets. The variable context is defined under the annotation @VARIABLECONTEXT. The options are given in the following format.

```
@VARIABLECONTEXT = "[{'name':'<variable-name-1>',
'<option-1-1>':'<value-1-1>', '<option-1-2>':'<value-1-2>', .....}, ..... {'name':'<variable-name-n>',
'<option-n-1>':'<value-n-1>', '<option-n-2>':'<value-n-2>', .....}]"
```

The possible options are explained in the table below

Option	Description
configuredvaluexpath	This specifies the Xpath (With reference to device XML), from which the value of the parameter has to be fetched.

Option	Description
	The behaviour is same as that of Configured value Xpath except that the value is given explicitly. This is considered only when 'configuredvaluexpath' is not specified.
	This contains the Xpath (with reference to device xml) to fetch the set of values for populating the options.
	This is same as selectionvalues except that the comma separated values are given explicitly.
parameterscope	<p>This is used to specify the scope of a parameter</p> <ul style="list-style-type: none"> • entityspecific – A value is required for each individual entity • devicespecific – A value is required for each individual device • global – A single value is got for all the entities

Local Script Execution

Junos Space can be used to trigger the execution of op scripts in one or more devices simultaneously without staging and enabling it. This can be done through the local script execution feature. Here the script will be executed locally in Junos Space server itself. Normal script is differentiated from local script by the @ISLOCAL annotation in the script. And it should have the value as 'true'.

```
/*@ISLOCAL="true"*/
```

Local scripts do not require stage/enable/disable actions as these scripts would be running directly in the Space server. If a script that is already deployed is modified with @ISLOCAL annotation the update will be rejected.

Local scripts can be executed by selecting one or more devices. Local scripts shall be executed in VIP node in case of a cluster setup.

If execution type is 'GROUPEDEXECUTION', Device IP address List is passed as a parameter. The script internally opens a connection before interacting with the device.



NOTE: Local scripts can be executed only for devices with space initiated connection.

Nesting variables

User can use XPath context to define the default option/selectable options of a variable (To be shown in the script execution screen. This XPath could have dependencies on other variables. Consider the example below:

of the selected Physical Interface(Input-1). We define a variable PHYINT to get the name of the physical interface and a variable LOGINT to get the name of the logical interface. We define the SELECTIONVALUESXPATh for PHYINT as `"/device/interface-information/physical-interface/name/text()"`. User can select a value from the options listed by the Xpath. Since the selection values listed for LOGINT variable

is dependent on the value selected for PHYINT, we can define the SELECTIONVALUESXPath of LOGIN as `"/device/configuration/interfaces/interface[name='$PHYINT']/unit/name/text()`". This ensures that, only the logical interfaces of the selected physical interface are listed.



NOTE: When using \$INTERFACE, \$UNIT, Configured Value Xpath, Invisible Params, Selection fields, the variable definition in the configlet editor should contain `.get(0)` in order to fetch the value from the array. Eg: `$INTERFACE.get(0)`

Related Documentation

- [Script Example on page 371](#)
- [Scripts Overview on page 275](#)

Script Example

The following is the script to take PIC offline.

A script has four associated attributes, @CONTEXT, @NAME, @DESCRIPTION and @CONFIRMATION. These attributes 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,"FPC")]/chassis-sub-module[starts-with(name,"PIC")] */
/* @NAME = "Put PIC Offline" */
/* @DESCRIPTION = "Take PIC offline." */
/* @CONFIRMATION = "Are you sure that you want to take the PIC offline?" */
/* @EXECUTIONTYPE = "SINGLEEXECUTION" */
/*@VARIABLECONTEXT="{['name':'XPATHVARIABLE1','defaultvalue':'mydefaultvalue',
'parameterscope':'devicespecific'},
{'name':'XPATHVARIABLE2','configuredvaluexpath':'/device/interface-information/
physical-interface/name/text()','parameterscope':'entityspecific'},
{'name':'XPATHVARIABLE3','selectionvaluesxpath':'/device/interface-information/
physical-interface/name/text()','parameterscope':'global'}]" */
/* 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 Annotations on page 367](#)
 - [Scripts Overview on page 275](#)

PART 6

Reports and Report Definitions

- [Report Definitions on page 375](#)
- [Reports on page 387](#)

Report Definitions

- [Reports Overview on page 375](#)
- [Creating Report Definitions on page 382](#)
- [Managing Report Definitions on page 383](#)

Reports Overview

You can use the Reports workspace to generate customized reports for managing the resources on your network. You can use these reports to gather data related to 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. Junos Space Network Management Platform provides some pre-defined categories to create report definitions. You can combine multiple categories to create a report definition. By default, a predefined 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 following predefined categories to create report definitions:

- **Audit Trail report definition** – This report definition allows you to view the audit log activities and tasks initiated on Junos Space Network Management Platform.
[Table 52 on page 376](#) lists the attributes available with this report definition.

Table 52: Audit Trail Report Definition Attributes

Attribute	Description
User Name	Login ID of the user who initiated the task
User IP	IP address of the client computer that the user used to initiate the task
Task	Name of the task that triggered the audit log
Timestamp	Time in the UTC time format in the database that is mapped to the local timezone of client computer
Result	Execution result of the task that triggered the audit log
Job ID	Job ID of the job-based task that is included in the audit log
Description	Description of the audit log logged on Junos Space Network Management Platform

- **Device Inventory report definition** – This report definition allows you to view the generic characteristics of all devices managed by Junos Space Network Management Platform.
[Table 53 on page 376](#) lists the attributes available with this report definition.

Table 53: Device Inventory Report Definition Attributes

Attribute	Description
Name	Name of the device
Configuration State	State of the configuration on a device
Vendor	Vendor of the device
IP Address	IP address of the device
Managed Status	Current status of the managed device in Junos Space Network Management Platform
Device Family	Device family of the selected device
OS Version	Operating system firmware version running on the device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Connection Status	Connection status of the device — whether UP or DOWN

Table 53: Device Inventory Report Definition Attributes (*continued*)

Attribute	Description
Schema Version	Junos OS configuration schema version on the device
Authentication Status	Mode of connecting the device to Junos Space Network Management Platform — whether key-based, credentials-based, or a key conflict
Serial Number	Serial number of the device
Connection Type	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. [Table 54 on page 377](#) lists the attributes available with this report definition.

Table 54: Device License Inventory Report Definition Attributes

Attribute	Description
Device Name	Name of the device
Feature Name	Name of the licensed SKU or feature
License Count	Number of times an item has been licensed
Used Count	Number of times the feature is used
Need Count	Number of times the feature is used without a license
Given	Number of instances of the feature that are provided by default
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	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. [Table 55 on page 378](#) lists the attributes available with this report definition.

Table 55: Device Logical Interface Inventory Report Definition Attributes

Attribute	Description
Device Name	Name of the device
Physical Interface	Name of the physical interface
Admin Status	Admin status of the interface — whether UP or DOWN.
Link Type	Type of the physical interface link—whether full duplex or half duplex
Logical Interface	Name of the logical interface
Logical Interface IP	IP address of the logical interface
Logical Encapsulation	Encapsulation used on the logical interface
VLAN	VLAN ID of the logical interface
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Device IP Address	IP address of the device
Physical Interface IP	IP address of the physical interface
MAC Address	MAC address of the physical interface
Operation Status	Operational status of the interface —whether UP or DOWN
Physical Encapsulation	Encapsulation used on the physical interface
Speed	Speed at which the interface is running (in Mbps)
MTU	Size of the MTU.
Description	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. [Table 56 on page 379](#) lists the attributes available with this report definition.

Table 56: Device Physical Interface Inventory Report Definition Attributes

Attribute	Description
Device Name	Name of the device
Physical Interface	Name of the physical interface
Admin Status	Admin status of the interface — UP or DOWN
Link Type	Type of the physical interface link —full duplex or half duplex
Link Level Type	type of the link level
IP Address	IP address of the physical interface
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
MAC Address	MAC address of the physical interface
Operation Status	Operational status of the interface, whether UP or DOWN
Encapsulation	Encapsulation used on the physical interface
Speed	Speed at which the interface is running (in Mbps)
MTU	Size of the MTU
Description	Description of the physical interface

- **Device Physical Inventory report definition** – Use this report definition to view the generic characteristics of the hardware modules for devices managed by Junos Space Network Management Platform. [Table 57 on page 379](#) lists the attributes available with this report definition.

Table 57: Device Physical Inventory Report Definition Attributes

Attribute	Description
Device Name	Name of the device
Chassis	Chassis component of the device
Module	Components contained in the chassis

Table 57: Device Physical Inventory Report Definition Attributes (*continued*)

Attribute	Description
Sub Module	Components contained in the submodule
Sub Sub Module	Components contained in the submodule of the submodule
Sub Sub Sub Module	Components contained in in the submodule of the submodule of the submodule
Model	Model name of the component
Model Number	Model number of the device component
Part Number	Part number of the chassis component.
Revision	Revision number of the component
Part Serial Number	Hardware serial number of the component
Status	Current operation status of the component
IP Address	IP address of the physical component
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Description	Description of the physical component



NOTE: You can filter the columns in device physical inventory report by using only tags. You can also sort and group the Device Name column only in the device physical inventory report.

- **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. [Table 58 on page 380](#) lists the attributes available with this report definition.

Table 58: Device Software Inventory Report Definition Attributes

Attribute	Description
Device Name	Device configuration name for the device
Package Name	Name of the software package installed on the device

Table 58: Device Software Inventory Report Definition Attributes (*continued*)

Attribute	Description
Version	Version number of the software package installed on the device
Type	Type of the the software package installed on the device
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Model	Model of the device
Routing Engine	Specific Routing Engine on a device supporting multiple Routing Engines
Description	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. [Table 59 on page 381](#) lists the attributes available with this report definition.

Table 59: Job Inventory Report Definition Attributes

Attribute	Description
ID	Numerical ID of the job
Name	Name of the job appended with the job ID
Percent	Percentage completion of the job
Job Type	Supported job types
State	State of job execution
Summary	Operations executed for the job
Scheduled Start Time	Start time specified for the job
User	Login name of the user who scheduled the job
Recurrence	Recurrence of the job
Retry Group ID	Job ID of the retry job
Actual Start Time	Time when the job started to execute

Table 59: Job Inventory Report Definition Attributes (*continued*)

Attribute	Description
End Time	Time the job ended
Previous Retry	Job ID of the previous retry job

When you add filter criteria for a column in a report definition, you can enter multiple filter values. You can separate filter values using commas. Columns that meet any of the filter values are listed in the report. The data types that support filtering using multiple filter values are String, Integer, Date, and Enum.

You can use the report definitions to generate reports in the CSV, HTML, and PDF formats. The reports display the name of the report and the description of the report. You can 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. You can also tag the reports and report definitions (See [“Tagging an Object” on page 793](#)).

- Related Documentation**
- [Creating Report Definitions on page 382](#)
 - [Generating Reports on page 387](#)

Creating Report Definitions

Report definitions specify 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, and the description of the report definition.

To create a report definition:

1. On the Junos Space Network Management Platform user interface, select **Reports > Report Definitions**.
2. Click the Create Report Definition icon from the Actions bar.

The Create Report Definition page is displayed.

3. In the **Report Name** field, type a user-defined report definition name.

A report definition name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quote ('), forward slash (/), and ampersand (&).

4. (Optional) In the **Description** field, type a user-defined description.

The description cannot exceed 256 characters.

5. Click the Add icon below the Description field.
The Select Categories window is displayed.
6. Select the check boxes next to the categories you want to add to the report definition.
7. Click **Add**.
8. Click the Pencil icon in the Filter 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 list to group the columns in the report definition in a specific order.
11. Select an appropriate option in the **Sort By** drop-down list 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 next to add filters in the report definition.
14. Select the appropriate column from the drop-down list for which you want to add a filter.
15. Select the appropriate operand corresponding to the column, from the drop-down list.
16. Type the criteria to be filtered.
17. Click **OK**.
18. Click **Create**.

You can use the report definition to generate reports. (See [“Generating Reports” on page 387](#)).



NOTE: You can view the reports generated from a report definition by clicking the View link in the Reports column corresponding to the report definition.

Related Documentation

- [Reports Overview on page 375](#)
- [Modifying Report Definitions](#)
- [Deleting Report Definitions](#)

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 384](#)
- [Cloning Report Definitions on page 384](#)
- [Deleting Report Definitions on page 384](#)
- [Viewing Report Definitions on page 384](#)

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 382](#)

CHAPTER 42

Reports

- [Generating Reports on page 387](#)
- [Viewing Generated Reports on page 388](#)
- [Deleting Generated Reports on page 389](#)

Generating Reports

You can generate reports from the report definitions you have created. The types of reports provided by Junos Space Network Management Platform are – 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. On the Junos Space Network Management Platform user interface, 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 Actions bar.

The Generate Reports window is displayed.

3. Select the appropriate report formats you want to generate by selecting the checkboxes next to the Report Format field.

Junos Space Network Management Platform provides reports in the CSV, HTML, fPDF and PDF 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 list, 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 **User Name** field, enter the username used to access the SCP server.
- e. In the **Password** field, enter the password 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 addresses you specify.
7. In the **Email Address** field, enter the email address.
8. Click **Add**.

You can add multiple email addresses if you want the report to be delivered to multiple email addresses.

9. Click the **Schedule at a later time** checkbox and schedule the date and time to generate the report automatically.
10. Click the **Recurrence** checkbox and specify the frequency to generate the report periodically.
11. Click **Generate**.

You can view, download, or print the reports. (See [“Viewing Generated Reports” on page 388](#)).

- Related Documentation**
- [Reports Overview on page 375](#)
 - [Creating Report Definitions on page 382](#)

Viewing Generated Reports

You can view the reports you have generated on the Generated Reports page in the Reports workspace. 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. On the Junos Space Network Management Platform user interface, select **Reports > Generated Reports**.

The list of generated reports are displayed in the tabular format.
2. Click the **View/Download** link corresponding to the report you want to view or download.
3. Click the format of the report you want to view and download.

- Related Documentation**
- [Reports Overview on page 375](#)
 - [Generating Reports on page 387](#)

Deleting Generated Reports

You can delete the reports you have generated from the Generated Reports page.

To delete the reports you have generated:

1. On the Junos Space Network Management Platform user interface, 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 Generated Report icon on the Actions bar.

The Delete Report window is displayed.

3. Click **Delete**.

Related Documentation

- [Reports Overview on page 375](#)
- [Generating Reports on page 387](#)

PART 7

Network Monitoring

- [Network Monitoring Overview on page 393](#)
- [Monitoring Devices and Assets on page 399](#)
- [Working With Events, Alarms, and Notifications on page 413](#)
- [Working With Reports and Charts on page 423](#)
- [Managing Network Monitoring System on page 431](#)
- [Managing Network Monitoring Operations on page 439](#)
- [Managing Devices on page 463](#)
- [Configuring Alarm Notifications on page 465](#)

CHAPTER 43

Network Monitoring Overview

- [Network Monitoring Workspace Overview on page 394](#)
- [Network Monitoring Reports Overview on page 397](#)

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: Junos Space Release 13.2 supports SNMP monitoring of devices using SNMP v1 and SNMPv2c.



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.

To grant a Junos Space user full privileges to access and perform tasks from the Network Monitoring workspace, the user must be assigned the FMPM Manager role. To grant a Junos Space user read-only access to the Network Monitoring workspace, the user must be assigned the FMPM Read Only User role.

The Network Monitoring workspace supports the following three types of users:

- **Administrator role:** A user assigned the FMPM Manager role and with access to Global domain can view and administer all devices in the Network monitoring workspace, including all devices that exist in other sub-domains.
- **Regular user role:** A user assigned the FMPM Manager role but without access to global domain can only view and administer devices in their selected domain. This type of user can also acknowledge and clear alarms.
- **Read only user role:** A user assigned the FMPM Read Only User role (or a customized role with FMPM access capability except admin tab) in Junos Space. This type of user can only view devices in the selected domain, but cannot access the **Network Monitoring > Admin** workspace and cannot acknowledge or clear alarms.

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. The following performance data is collected:

- *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 and 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 399](#)).
- **Search:** Search for devices (see [“Searching in the Network Monitoring Workspace” on page 402](#)).
- **Outages:** View unavailable (down) services (see [“Viewing and Tracking Outages” on page 413](#)).
- **Events:** View events (see [“Viewing and Managing Events” on page 414](#)).
- **Alarms:** View alarms (see [“Viewing and Managing Alarms” on page 97](#)).

- Notifications: Display notices received by users (see [“Viewing, Configuring, and Searching for Notifications” on page 421](#)).
- Assets: Search asset information and assets inventory (see [“Tracking and Searching for Assets” on page 405](#)).
- Reports: View reports (see [“Viewing Reports” on page 424](#)).
- Charts: View charts (see [“Viewing Charts” on page 429](#)).
- Topology: View nodes in the network topology and the events and alarms associated with the nodes (see [“Working with Topology” on page 406](#)).
- Admin: Perform system administration (see [“Admin: Configuring Network Monitoring” on page 431](#)).

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 (12.3 or 13.1) to 13.2 allows a means to preserve the custom configuration that might have been performed on XML files from the backend automatically. For example, assume that you have modified or customized the SNMP poll interval in the `collectd-configuration.xml` in Junos Space Platform Release 12.3 or 13.1, that is, before upgrade to 13.2. When you upgrade to Release 13.2, the upgrade process automatically recognizes the changes made and preserves the changes in the 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 397](#)
- [Updating Network Monitoring After Upgrading the Junos Space Network Management Platform on page 433](#)

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 397](#)
- [Key SNMP Customized Performance Reports, Node Reports, and Domain Reports on page 397](#)
- [Database Reports on page 397](#)
- [Statistics Reports on page 397](#)

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 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 394](#)
- [Creating Reports on page 423](#)
- [Deleting Reports on page 429](#)
- [Viewing Reports on page 424](#)

- [Viewing the Node List on page 399](#)

Monitoring Devices and Assets

- [Viewing the Node List on page 399](#)
- [Resyncing Nodes on page 400](#)
- [Turning SNMP Data Collection Off and On on page 401](#)
- [Searching in the Network Monitoring Workspace on page 402](#)
- [Viewing the Dashboard on page 403](#)
- [Tracking and Searching for Assets on page 405](#)
- [Working with Topology on page 406](#)

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 400](#)).

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



NOTE: In Junos Space Network Management Platform Release 13.3, you cannot modify surveillance categories.

- [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 and asset information; and rescan, access the admin options, and schedule outages.

Related Documentation

- [Network Monitoring Workspace Overview on page 394](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Viewing and Managing Alarms on page 97](#)
- [Viewing, Configuring, and Searching for Notifications on page 421](#)
- [Tracking and Searching for Assets on page 405](#)

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 14](#)).

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 394](#)
- [Viewing the Node List on page 399](#)
- [Turning SNMP Data Collection Off and On on page 401](#)
- [Viewing Managed Devices on page 14](#)

Turning SNMP Data Collection Off and On



NOTE: In Junos Space Network Management Platform Release 13.3, you cannot modify surveillance categories; therefore, the content in this topic is not applicable for Release 13.3.

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. However, turning on data collection increases the amount of SNMP traffic. 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 457](#)). 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 440](#).

- Related Documentation**
- [Viewing the Node List on page 399](#)
 - [Searching in the Network Monitoring Workspace on page 402](#)
 - [Viewing the Dashboard on page 403](#)

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, including address, circuit ID, date installed, lease expiry date, and 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 six 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 394](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)

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).



NOTE: In Junos Space Network Management Platform Release 13.3, you cannot modify surveillance categories.

If your dashboard does not display information about all your nodes, you should resynchronize your nodes. See [“Resyncing Nodes” on page 400](#).

Under the Show all nodes heading, each of the items—Routers, Switches, Security Devices, Media Flow Controllers, 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 60 on page 404 displays the alarms.

Table 60: 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 61 on page 404 displays the notifications.

Table 61: 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	User who received the notification.
Response Time	The time it took to respond.

Table 62 on page 405 displays the status of the node.

Table 62: 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 63 on page 405 displays the resource graphs information:

Table 63: 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 401](#)
- [Resyncing Nodes on page 400](#)

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.

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 the **All nodes with asset info** link.

**Related
Documentation**

- [Network Monitoring Workspace Overview on page 394](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Searching in the Network Monitoring Workspace on page 402](#)

Working with Topology

From the topology map, you can view nodes (Junos Space physical or virtual appliances) added to the Junos Space Network Management Platform fabric and devices discovered in the Junos Space Network Management Platform.

By default, the node with the highest "bandwidth" (which takes the number of interfaces and adds all their ifspeeds) gets displayed in topology page.

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.

To view the management IP, name, and current status for any device in the topology, place the mouse cursor over the node link. When you select a node link on the topology, the link is highlighted. You can select multiple nodes by pressing Ctrl. You can use the zoom slider to zoom in and zoom out of the selected topology view. You can also use the semantic zoom-level functionality on the topology map to display nodes one or more hops away from the selected nodes.

- [Using the Search Option to View Nodes on page 407](#)
- [Working with Topology Map Views on page 407](#)
- [Viewing Alarms and Node Details for Nodes on page 408](#)
- [Viewing Nodes with Active Alarms on page 409](#)
- [Managing Alarms Associated with Nodes on page 410](#)
- [Viewing the Topology Map with Different Layouts on page 410](#)
- [Automatic Refresh of Topology Map on page 410](#)
- [Pinging a Node on page 411](#)
- [Viewing the Alarms Associated with the Node on page 411](#)

- [Viewing the Events Associated with the Node on page 411](#)
- [Viewing the Resource Graphs Associated with the Node on page 412](#)

Using the Search Option to View Nodes

You can use the Search option to view nodes in the topology map based on the text you enter in the search field, for example:

- Enter **Nodes** in the Search field to select nodes from the list of all available nodes in the network topology.
- Enter **Category** in the Search field to select nodes by device category (Routers, Switches, Security Devices, and so forth).



NOTE: Categories can be collapsed and expanded.



NOTE: To display all nodes in the network topology, select the Monitor_SNMP category.

- Enter the name of a specific device in the search window to display a specific device.

Working with Topology Map Views

From the **Network Monitoring > Topology** page, you can use the topology map options described in [Table 64 on page 407](#) to view and manage nodes:

Table 64: Topology Map Options

Option	Description
Click to go back button	View the previous topology view history.
Click to go forward button	View the more recent topology view history, after viewing the past history.
Center on Selection button	Display the selected nodes in the center of the topology view.
Show Entire Map button	Display all the (filtered) nodes in the topology view.
Toggle Highlight Focus Nodes button	When you add a node to focus, nodes connected to the focus node might also be displayed. When you click the Toggle Highlight Focus Nodes button, only focus node icons are highlighted, and icons are dimmed for non-focus nodes that are connected to the focus nodes.
Zoom slider	Move the slider up (+) to zoom in or down (–) to zoom out.
Pan Tool button	Select on a node to reposition in topology view, or select between nodes (in white space) to pan all nodes in the topology view (up, down, left, or right) as a single image. To disable the Pan Tool function, click the Selection Tool button.

Table 64: Topology Map Options (*continued*)

Selection Tool button—	Perform operations on individual nodes (add node to focus, ping node, view node information, view events/alarms, and so forth). To disable the Selection Tool function, click the Pan Tool button.
Expand Semantic Zoom Level/Collapse Semantic Zoom Level	Expand or collapse the semantic zoom level by using the Up arrow key to increase the hop count or the Down arrow key to decrease the hop count. For example, select a hop count of 2 to display the network nodes two hops away from the focus nodes. NOTE: The topology view displays a line to show connections to nodes that are one or more hops away from a focus node.
Refresh Now button	Right-click inside the topology map (without selecting on a node) to refresh the status of nodes in the topology view.

Viewing Alarms and Node Details for Nodes

To view details for a category of nodes or selected nodes:

1. Select **Network Monitoring > Topology**.

By default, the node with the highest "bandwidth" (which takes the number of interfaces and adds all their ifSpeeds) gets displayed in topology page.

2. From the topology view, select a category of nodes or click on the nodes you want to view.

- To view alarm details for a category of nodes or selected nodes, select the **Alarms** tab.

The following alarm details are displayed:

- 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—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.
- Log Message—The log message associated with the alarm.

- To view node details for the category of nodes or selected nodes, select the **Nodes** tab.

The following nodes details are displayed:

- ID
- Creation Time
- Foreign ID

- Foreign Source
- Label
- Last Capabilities Scan
- Primary interface
- sysContact
- sysDescription
- sysLocation

3. To view more in-depth information about a node, right-click on the node and select **Node Info**.

The Node Info page displays complete information about the events and alarms associated with the node:

- General Status
- Node availability (last 24 hours)
- Node interfaces (IP and physical interfaces)
- Notification (Outstanding/Acknowledged)
- Recent events
- Recent outages
- SNMP attributes
- Surveillance Category Memberships



NOTE: In Junos Space Network Management Platform Release 13.3, you cannot modify surveillance categories.

Viewing Nodes with Active Alarms

To view nodes with active alarms:

1. Select **Network Monitoring > Topology**.
2. Use the Search option to select the nodes you want to check for active alarms.

In the topology view, the color of the node icon indicates the highest severity alarm associated with the node. In addition, the node icon displays a number that indicates the count of outstanding alarms and notices associated with that node.



NOTE: A node with an active alarm of "Major" severity displays a red icon.

Managing Alarms Associated with Nodes

To acknowledge, unacknowledge, escalate, or clear the alarms associated with a node:

1. Select **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, or click **Select All** to manage all the listed alarms.
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.

Viewing the Topology Map with Different Layouts

To view the topology map with different layouts:

1. Select **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

Automatic Refresh of Topology Map

By default, the topology map view is not automatically refreshed. To initiate an automatic refresh of the topology map:

1. Select **Network Monitoring > Topology**.
2. Select the **View** menu and then select **Automatic Refresh**.

The topology map is automatically refreshed every 60 seconds.

Pinging a Node

To ping a node:

1. Select **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 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 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 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.

Related Documentation

- [Network Monitoring Workspace Overview on page 394](#)
- [Resyncing Nodes on page 400](#)

CHAPTER 45

Working With Events, Alarms, and Notifications

- [Viewing and Tracking Outages on page 413](#)
- [Viewing and Managing Events on page 414](#)
- [Viewing and Managing Alarms on page 417](#)
- [Viewing, Configuring, and Searching for Notifications on page 421](#)

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 on 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 394](#)
- [Viewing the Node List on page 399](#)

- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)

Viewing and Managing Events

By default, the Junos Space Network Management Platform is monitored using the built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Monitoring > Node List), and referred to hereafter as the 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 that take you back to previous pages. Listings frequently extend over multiple pages, among 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 414](#)
- [Advanced Event Search on page 415](#)
- [Viewing the Events List on page 415](#)
- [Viewing Event Details on page 416](#)
- [Using Event Filters to View Events on page 417](#)

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 415](#).
- 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 416](#).
- To perform an advanced search, click **Advanced Search** to go to the Advanced Event Search section. Use the Advanced Event Search section to search the event list on multiple fields. See [“Advanced Event Search” on page 415](#).

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

To display a list of events, select **Network Monitoring > Events** and click **All events** in the Event Queries section. 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 415](#)).
- 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 416](#)).
- **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 402](#)). 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 402](#)). 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**—The 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 446](#)).
- **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 the 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 the 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.

Using Event Filters to View Events

If you previously created event filters, you can select a filter from Event Filter Favorites. Only those events that match the filtering criteria specified in the user-defined event filter are displayed.

To select an event filter to view events:

1. Navigate to **Network Monitoring > Events** and select a filter from Event Filter Favorites.
The events that match the filtering criteria specified in the event filter are displayed.
2. To clear the filter and reset all event-filtering criteria, select **Remove Filter**.
All outstanding events are displayed (the default view).

Related Documentation

- [Network Monitoring Workspace Overview on page 394](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Searching in the Network Monitoring Workspace on page 402](#)
- [Managing Event Filters](#)

Viewing and Managing Alarms ---

By default, the Junos Space Network Management Platform is monitored using a built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Monitoring > Node List), and is referred to as the Junos Space Network Management Platform node.

There are two 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, or unacknowledged an alarm, the detailed alarm view displays *admin* instead of the actual remote user in the Acknowledged By field.

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 418](#)
- [Using Alarm Filters to View Alarms on page 420](#)
- [Acknowledging Alarms on page 420](#)
- [Clearing Alarms on page 420](#)
- [Escalating Alarms on page 421](#)
- [Unacknowledging Alarms on page 421](#)
- [Viewing Acknowledged Alarms on page 421](#)

Viewing Alarms

To view alarms:

1. Select **Network Monitoring > Alarms**.
2. Select from any of the following links:
 - All alarms (summary)
 - All alarms (detail)
 - Advanced Search
 - NCS Alarm List

The Alarms page displays 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 16 on page 99](#) 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 65: 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 ID section of the Alarms page.
Severity	Color-coding only	X	Toggle to show only alarms with this severity, or not to show alarms with this severity.
UEI		X	Toggle to show only events with this UEI, or not to show events with this UEI.
Node	X	X	Toggle 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. Toggle to show only alarms occurring after this event, or only alarms occurring before this event.

Table 65: Information Displayed in the Alarms List (*continued*)

Data	Short Listing	Long Listing	Comments
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.

Using Alarm Filters to View Alarms

If you previously created alarm filters, you can select a filter from Alarm Filter Favorites to display the alarms that match the filtering criteria specified in the alarm filter.

To select an alarm filter to view alarms:

1. Navigate to **Network Monitoring > Alarms** and select a filter from Alarm Filter Favorites.
The alarms that match the filtering criteria specified in the alarm filter are displayed.
2. To clear the filter and reset all alarm filtering criteria, select **Remove Filter**.
All outstanding alarms are displayed (the default view).

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 421](#)
- [Managing Alarm Filters](#)

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 e-mail 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 431](#)), 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 422](#)

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 431](#).

Related Documentation

- [Network Monitoring Workspace Overview on page 394](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Searching in the Network Monitoring Workspace on page 402](#)

CHAPTER 46

Working With Reports and Charts

- [Creating Reports on page 423](#)
- [Viewing Reports on page 424](#)
- [Deleting Reports on page 429](#)
- [Viewing Charts on page 429](#)

Creating Reports

You can configure key SNMP customized (KSC) performance reports, node reports, and domain reports by selecting **Network Monitoring > Reports**.

- [Creating Key SNMP Customized Performance Reports, Node Reports, and Domain Reports on page 423](#)
- [Creating a New KSC Report from an Existing Report on page 424](#)

Creating Key SNMP Customized Performance Reports, Node Reports, and 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:
 - a. Select **Add New Graph**.
 - b. Select a resource from the Resources section.
 - c. Select **Choose Child Resource** to select the resource you want to use in a graph.
 - 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.
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 394](#)
- [Network Monitoring Reports Overview on page 397](#)
- [Viewing Reports on page 424](#)
- [Deleting Reports on page 429](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)

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, and 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, or custom) that the report should cover.

The statistical data is refreshed to reflect the time period specified.

Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, and 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 the 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 the 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 e-mail report check box.
- f. In the format field, select the format type (HTML, PDF, or 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 394](#)
- [Network Monitoring Reports Overview on page 397](#)
- [Creating Reports on page 423](#)
- [Deleting Reports on page 429](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Searching in the Network Monitoring Workspace on page 402](#)

Deleting Reports

To delete key SNMP customized (KSC) reports and database reports, select **Network Monitoring > Reports**.

- [Deleting Key SNMP Customized Reports on page 429](#)
- [Deleting Pre-Run Database Reports on page 429](#)

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 394](#)
- [Network Monitoring Reports Overview on page 397](#)
- [Creating Reports on page 423](#)
- [Viewing Reports on page 424](#)
- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Searching in the Network Monitoring Workspace on page 402](#)

Viewing Charts

To view charts, select **Network Monitoring > Charts**.

By default, this page displays:

- 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 431](#)
- [Updating Network Monitoring After Upgrading the Junos Space Network Management Platform on page 433](#)

Admin: Configuring Network Monitoring

You can view the network monitoring configuration and the system configuration on which network monitoring is running and generate network monitoring log reports for troubleshooting purposes.

This topic contains the following tasks:

- [Network Monitoring System: System Information on page 431](#)
- [Generating a Log File for Troubleshooting on page 432](#)
- [Notification Status on page 432](#)

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

Generating a Log File for Troubleshooting

To generate a log report for troubleshooting purposes:

1. Select one or more of the following plugins that you want to enable for reporting purposes:
 - Java: Java and JVM information
 - OS: Kernel, OS, and Distribution
 - Network monitoring: network monitoring core information, version, or basic configuration
 - TopEvent: Top 20 most reported events
 - Threads: Java thread dump (full output only)
 - Top: Output of the 'top' command (full output only)
 - Isof: Output of the 'Isof' command
 - Configuration: Append all network monitoring configuration files (full output only)
 - Logs: network monitoring log files (full output only)
2. Select the report type (text or zip file) to be generated.
3. Select **Submit Query**
4. You can view or save the file:
 - To view the report file, click **Open** from the File Download dialog box.
 - To save the report, click **Save** from the File Download dialog box.

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 394](#)

- [Viewing the Node List on page 399](#)
- [Viewing Managed Devices on page 14](#)
- [Resyncing Nodes on page 400](#)
- [Searching in the Network Monitoring Workspace on page 402](#)
- [Viewing, Configuring, and Searching for Notifications on page 421](#)

Updating Network Monitoring After Upgrading the Junos Space Network Management Platform

- [Overview on page 433](#)
- [Step 1: Monitoring the Software Install Status Window for File Conflicts on page 433](#)
- [Step 2: Identifying Files with Conflicts on page 434](#)
- [Step 3: Merging Files with Conflicts on page 436](#)
- [Step 4: Verifying the Manual Merge Status of Configuration Files on page 437](#)
- [Step 5: Final Steps After Upgrading Network Monitoring on page 437](#)

Overview

After upgrading the Junos Space Network Management Platform, the Network Monitoring configuration files might not contain the configuration file changes for the latest version. During the Junos Space Network Management upgrade process, the Software Install Status window displays a message if there are any configuration files in conflict. You can also access the `/var/log/install.log` file to view any files that have conflicts. To manually merge files that contain conflicts, you must perform all of the following steps. When the upgrade process encounters no files in conflict, the files are auto-merged and you do not need to perform the following steps.

Step 1: Monitoring the Software Install Status Window for File Conflicts

Check for the following message in the Software Install Status window during the upgrade of the Junos Space Network Management Platform:

```
WARNING: Conflict observed during OpenNMS git-merge so please merge the
changes manually:
Please go to folder /opt/opennms/etc, and merge the *.old.bak files to
current running files.
```

When logged in from the Junos Space Network Management Platform command-line interface (CLI), you can also check for file conflicts from the `/var/log/install.log` file. The following example message from the `install.log` file shows three files with conflicts that you will need to manually merge to resolve:

```
opennms-post.pl 62: Error while running git merge
opennms-auto-upgrade/pristine: merge -Xpatience
-Xignore-space-change -Xignore-all-space -Xnormalize
opennms-auto-upgrade/pristine:
command returned error: 1 at /usr/lib/perl5/site_perl/5.8.8/Error.pm line
343.
```

opennms-post.pl 63: The following files are in conflict:

opennms-post.pl 65: eventconf.xml

opennms-post.pl 65: events/ncs-component.events.xml

opennms-post.pl 65: linkd-configuration.xml



NOTE: If no files with conflicts are found during the upgrade process, the files are automatically merged, and you do not need to perform any additional steps. Otherwise, you must complete each of the following steps.

Step 2: Identifying Files with Conflicts

If you discovered one or more files with conflicts during the previous step, perform the following steps to identify the files with conflicts:

1. Log in to the virtual IP (VIP) fabric node.
2. Stop the Network Monitoring service from the Junos Space Network Management Platform user interface:
 - a. Select **Network Management Platform > Administration > Applications**.
The Applications page appears.
 - b. Right-click **Network Management Platform** and click **Manage Services**. (Alternatively, you can select **Network Management Platform** and click **Manage Services** from the Actions menu.)
The Manage Services page is displayed.
 - c. Select the **Network Monitoring** service and click the **Stop Service** icon.
The **Confirm Stop SNMP Agent** dialog box is displayed.
 - d. Click **Yes**.
A status dialog box with a message indicating that the service has stopped is displayed.
 - e. Click **OK**.
A dialog box is displayed confirming that the service has successfully stopped.
 - f. Click **OK**.
You are taken to the Manage Services page.
3. From the Junos Space Network Management Platform CLI, check the status of the Network Monitoring service by executing the following command:

```
# su - opennms -c '/sbin/service opennms status'
```

Junos Space displays the message **opennms is stopped**.

4. To re-merge the Network Monitoring configuration files:
 - a. From the Junos Space CLI, execute the following command:

```
# /opt/opennms/bin/config-tools/conflict-remerge.pl
```

Junos Space displays output similar to the following:

```
conflict-remerge.pl 19: Resetting tree to
'opennms-auto-upgrade/tags/runtime/pre-1.13.0-0.20131227.1'
```

- b. Navigate to the **/opt/opennms/etc** directory and execute the following command:

```
# git status
```

Most of the files are auto-merged. If any files remain, the status of each file in conflict is displayed under the section "Unmerged paths" and is marked "both modified", as shown in the following example:

```
Unmerged paths:
```

```
# (use "git add/rm ..." as appropriate to mark resolution)
```

```
# both modified: eventconf.xml
```

```
# both modified: events/ncs-component.events.xml
```

```
# both modified: linkd-configuration.xml
```

For each remaining conflicted file (listed under Unmerged paths) changes that were made to the file are identified with the opening statement "**<<<<<< HEAD**" and closing statement "**>>>>>> opennms-auto-upgrade/pristine**". For example, in the **ncs-component.events.xml** file shown above, the file changes are marked as follows:

```
<<<<<< HEAD
```

```
<alarm-data-reduction
key="%uei:%parm[componentType]%%:parm[componentForeignSource]%%
:%parm[componentForeignId]%" alarm-type="2"
```

```
clear-
```

```
key="%uei.opennms.org/internal/ncs/componentImpacted:%parm[componentType]%%
:%parm[componentForeignSource]%%:parm[componentForeignId]%"
auto-clean="false"/>
```

```
=====
```

```
<alarm-data-reduction-
```

```
key="%uei:%parm[componentType]%%:parm[componentForeignSource]%  
:%parm[componentForeignId]%%:parm[nodeid]%" alarm-type="2"  
  
clear-  
  
ei.opennms.org/internal/ncs/componentImpacted:%parm[componentType]%  
:%parm[componentForeignSource]%%:parm[componentFo  
  
]:%parm[nodeid]%"  
  
auto-clean="false"/>  
  
>>>>>> opennms-auto-upgrade/pristine
```

Step 3: Merging Files with Conflicts

After identifying the files with conflicts, you must perform the following steps to manually merge each of the files and resolve all conflicts:

1. From a VI editor, open the file with conflicts.
2. Search for the statement "HEAD".
3. Identify the differences between the two configurations which are contained between the lines <<<<< HEAD and >>>>> opennms-auto-upgrade/pristine.
 - a. The configuration for the file *before* the upgrade is contained between the lines <<<<< HEAD and =====.
 - b. The configuration for the file *after* the upgrade is contained between the lines ===== and >>>>> opennms-auto-upgrade/pristine.
4. Save the configuration of the file *after* the upgrade, and then update it with any user-modified values from the configuration file *before* the upgrade.
5. After manually merging configuration file changes, remove each of the following lines from the file:

```
<<<<<< HEAD  
  
=====
```

```
>>>>>> opennms-auto-upgrade/pristine
```

6. Save the configuration file.
7. Repeat steps 2 through 6 for each configuration file with conflicts until all file conflicts in all files are merged.

After all the file conflicts are merged, there should be no occurrence of the following lines:

```
<<<<<< HEAD
```

```
=====
```

```
>>>>>> opennms-auto-upgrade/pristine
```

Step 4: Verifying the Manual Merge Status of Configuration Files

From the Junos Space CLI, execute the following commands to verify that the configuration file changes are merged correctly:

```
/opt/opennms/bin/config-tools/conflict-resolve.pl
```

```
git status
```

If the file changes were merged correctly, Junos Space displays the following message:

```
nothing to commit (working directory clean)
```

Step 5: Final Steps After Upgrading Network Monitoring

Perform the following steps after upgrading Network Monitoring:

1. Update permissions of the **/opt/opennms** directory to **774**:

```
# chmod -R 774 /opt/opennms
```

2. Run the following command to change the ownership of the **/opt/opennms** directory to **opennms:space**:

```
#chown -R opennms:space /opt/opennms
```

3. Verify that the **opennms.conf** file includes the line **RUNAS="opennms"**:

```
# more opennms.conf
```

```
START_TIMEOUT=0
```

```
ADDITIONAL_MANAGER_OPTIONS="-Djava.io.tmpdir=/opt/opennms/tmp -d64  
-XX:MaxPermSize=512m -
```

```
XX:HeapDumpPath=/var/opennms/java_pid <pid>.hprof  
-XX:+HeapDumpOnOutOfMemoryError -XX:+PrintGCTimeStamps  
-XX:+PrintGCDetails"
```

```
JAVA_HEAP_SIZE=2048
```

```
RUNAS="opennms" #####Verify that this line exists
```

4. The password of the user "postgres" in the **opennms-datasources.xml** file will be empty. Set the password to **postgres**:

```
<jdbc-data-source name="opennms-admin"
```

```
database-name="template1"
```

```
class-name="org.postgresql.Driver"
```

```
url="jdbc:postgresql://localhost:5432/template1"
```

```
user-name="postgres"
```

```
password="postgres" /> #####Password is set here
```

5. Start the Network Monitoring service from the Junos Space user interface:

- a. Select **Network Management Platform > Administration > Fabric**.

The Fabric page appears.

- b. Select the check box for each fabric node on which you want to start SNMP monitoring.

- c. From the **Actions** menu, select **SNMP Start**.

The **Confirm Start SNMP Agent** dialog box is displayed.

- d. Click **Yes**.

Junos Space starts SNMP monitoring on the selected fabric nodes.

6. If your fabric is running in a multi-node setup, execute the following command to verify that all the modified configuration files are synchronized across the standby node:

```
# /opt/opennms/contrib/failover/scripts/sync.sh
```

**Related
Documentation**

- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Managing Services on page 718](#)

Managing Network Monitoring Operations

- [Configuring SNMP Community Names by IP on page 439](#)
- [Configuring SNMP Data Collection per Interface on page 440](#)
- [Managing and Unmanaging Interfaces and Services on page 441](#)
- [Managing Thresholds on page 441](#)
- [Selecting and Sending an Event to the Network Management System on page 445](#)
- [Configuring Notifications on page 446](#)
- [Configuring Scheduled Outages on page 449](#)
- [Compiling SNMP MIBs on page 450](#)
- [Managing Events Configuration Files on page 455](#)
- [Managing SNMP Collections on page 457](#)
- [Managing Data Collection Groups on page 458](#)

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 this procedure, you enter 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 addresses 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 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 address 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 457](#)

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 notification, 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 441](#)
- [Modifying Thresholds on page 444](#)
- [Deleting Thresholds on page 445](#)

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, or 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 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, or 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 394](#)

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 446](#)
- [Configure Destination Paths on page 448](#)
- [Configure Path Outages on page 449](#)

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—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 394](#)

Configuring Scheduled Outages

You can configure scheduled outages to suspend notifications, polling, thresholding, and data collection (or any combination of these) for any interface or 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 450](#)
- [Compiling MIBs on page 451](#)
- [Viewing MIBs on page 451](#)
- [Deleting MIBs on page 451](#)
- [Clearing MIB Console Logs on page 452](#)
- [Generating Event Configuration on page 452](#)
- [Generating a Data Collection Configuration on page 453](#)

Uploading MIBs

To upload a MIB file:

1. Select **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 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 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 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 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 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 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**.
 - 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 is 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 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 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 394](#)

Managing Events Configuration Files

- [Adding New Events Configuration Files on page 455](#)
- [Deleting Events Configuration Files on page 456](#)
- [Modifying Events Configuration Files on page 456](#)

Adding New Events Configuration Files

To add a new events configuration file:

1. Select **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 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 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 394](#)

Managing SNMP Collections

- [Adding a New SNMP Collection on page 457](#)
- [Modifying an SNMP Collection on page 458](#)

Adding a New SNMP Collection

To add a new SNMP collection:

1. Select **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**.

Modifying an SNMP Collection

To modify an SNMP collection:

1. Select **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 394](#)

Managing Data Collection Groups

- [Adding New Data Collection Files on page 458](#)
- [Deleting Data Collection Files on page 459](#)
- [Modifying Data Collection Files on page 459](#)

Adding New Data Collection Files

To add a new data collection file:

1. Select **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 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 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 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 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 to which you want to associate this system definition, 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 394](#)

Managing Devices

- [Managing Surveillance Categories on page 463](#)

Managing Surveillance Categories



NOTE: In Junos Space Network Management Platform Release 13.3, you cannot modify surveillance categories; therefore, the content in this topic is not applicable for Release 13.3.

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 463](#)
- [Deleting Surveillance Categories on page 463](#)
- [Adding Surveillance Categories on page 464](#)

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 401](#)
- [Network Monitoring Workspace Overview on page 394](#)

CHAPTER 50

Configuring Alarm Notifications

- [Alarm Notification Configuration Overview on page 465](#)
- [Configuring Alarm Notification on page 468](#)

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 465](#)
- [Guidelines for Configuring Alarm Notifications on page 466](#)
- [Advanced Filtering on page 466](#)

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 468](#)

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 468](#)
- [Activating Alarm Notification Configuration Files for Basic Filtering on page 469](#)
- [Reloading a Filter Configuration to Apply Filter Configuration Changes on page 470](#)

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 `/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 465](#)

PART 8

Configuration Files

- [Manage Configuration Files on page 473](#)
- [Backup Config Files on page 487](#)

Manage Configuration Files

- [Managing Configuration Files Overview on page 473](#)
- [User Privileges in Configuration File Management Overview on page 475](#)
- [Viewing Configuration File Statistics and Inventory on page 476](#)
- [Deleting Configuration Files on page 477](#)
- [Restoring Configuration Files on page 478](#)
- [Comparing Configuration Files on page 480](#)
- [Editing Configuration Files on page 482](#)
- [Exporting Configuration Files on page 484](#)

Managing Configuration Files Overview

Centralized configuration file management enables you to maintain multiple versions of your device configuration files within Junos Space Network Management Platform. This helps you recover device configuration files in case of a system failure and maintain consistent configuration across multiple devices.



NOTE: Each commit command on a device creates a new version on the device, but no more than 49 versions can be stored on a device. However, Junos Space Network Management Platform provides backups with longer life-cycles, which helps you to verify or use a backup content that was created earlier than 49 versions.

Version management for configuration files in Junos Space Network Management Platform is therefore independent from configuration file versioning on devices. That is, a user can store more than 49 versions of a configuration file on the Junos Space server.

The configuration file management workspace handles the following types of configuration files:

- **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. When you execute a commit command, a backup configuration file is created and the oldest backup file (Version 49) is deleted on the device. The most recent backup configuration file is labeled Version 1.

The following is a potential workflow for an individual file or device in this workspace:

1. Back up the device configuration file and thus bring the device's running configuration under Junos Space Network Management Platform management.
2. Edit a copy of the backup configuration file to create a candidate configuration file.
3. Verify edits by comparing the initial backup version of the configuration file with the edited version.
4. Restore the candidate configuration file to the device.
5. Export the initial backup version to a zip file
6. Delete the initial backup version from Junos Space Network Management Platform.

Stored configuration files can be viewed by double-clicking the item on the Config Files Management page. A dialog box appears, displaying the stored configuration files in noneditable format. You can select the version that you want to view from the **Version** list. The timestamp is displayed adjacent to the version number and indicates the time at which the configuration was last backed up.

The status bar near the bottom of the dialog box shows the current page number and the total number of pages in the file. It also provides paging controls and a Refresh button. Use the **Show items** list to manage the number of lines of configuration displayed on a single page. By default, 50 lines are displayed. You can choose to display 200, 800, 3200, or 10,000 lines.

Below the device configuration is the Comments area. By default, for the initial backup file, you see the following comment in the Comments area:

This version of the Config file is imported from the device.

However, for an edited configuration file, this area displays the following comment:

This is an edited version of the configuration file version: x, where x represents the version of the configuration that you edited.

To perform an action on a configuration file, select a configuration file and then perform one of the following actions:

- Click an icon at the top of the Config Files Management page.
- Select an action from the Actions menu.
- Right-click and select an action.

On the Config Files Management page, you can perform the following actions:

- [Backing Up Configuration Files on page 488](#)
- [Deleting Configuration Files on page 477](#)
- [Restoring Configuration Files on page 478](#)
- [Comparing Configuration Files on page 480](#)
- [Editing Configuration Files on page 482](#)
- [Exporting Configuration Files on page 484](#)

**Related
Documentation**

- [Viewing Configuration File Statistics and Inventory on page 476](#)
- [User Privileges in Configuration File Management Overview on page 475](#)

User Privileges in Configuration File Management Overview

In Junos Space Network Management Platform, **Configuration File Manager** is the predefined role for configuration file management. With the Configuration File Manager role, you can perform the following tasks:

- Backup configuration files
- Delete configuration files
- Restore configuration files
- Compare configuration file Versions
- Export configuration files
- Modify configuration files

To restrict the Configuration File Manager permissions to only some of the preceding tasks, create a role and then assign permissions specifically for each list item. For more information about creating a user-defined role, see [“Creating a User-Defined Role” on page 553](#).

**Related
Documentation**

- [Managing Configuration Files Overview on page 473](#)
- [Role-Based Access Control Overview on page 519](#)

Viewing Configuration File Statistics and Inventory

The Configuration Files statistics page, which is directly under the Configuration Files workspace, displays two bar charts that provide the following information:

- Configuration file count by device family
- Devices with most frequently revised configuration files

In both cases, mouse over the bar charts to display information in a tooltip, such as number of configuration file versions for a device and so on.

All configuration files in Junos Space Network Management Platform are displayed on the **Config Files Management** page. You can view stored configurations by double-clicking an entry in tabular view.

The following information appears for each configuration file:

- **Config File Name**—Name of the configuration file, which has the .conf extension
- **Device Name**—Name or IP address of the device whose configuration is backed up
- **Latest ConfigFile Version**—Latest version number of the configuration file
- **Creation Date**—Timestamp when version 1 of the configuration file is created on the Junos Space server. It corresponds to the time at which you back up a device configuration for the first time from the Junos Space server.
- **Last Updated Date**—Timestamp when the device configuration is last modified

When you modify the device configuration, this action results in the addition of a newer version of the configuration file. Therefore, this timestamp corresponds to the time at which the latest version of the configuration file is created on the Junos Space server.



NOTE: If a column is not displayed by default, then click the down arrow next to a displayed column and select the desired column from the **Columns** list.

Related Documentation

- [Backing Up Configuration Files on page 488](#)
- [Managing Configuration Files Overview on page 473](#)
- [Tags Overview on page 780](#)

Deleting Configuration Files

You may want to delete the device configuration files from the Junos Space Network Management Platform in the following scenarios:

- When you want to use the device for a totally different purpose. In this case, because the configuration may have changed considerably, you cannot use the old backup configuration files to restore the device configuration.
- When the backup configuration file contains incorrect configuration information.

To delete a configuration file:

1. On the Junos Space Network Management Platform user interface, 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 configuration files of devices that you want to delete and click the **Delete Configuration Files** icon.

A message appears, asking you to confirm deletion.



CAUTION: Before you proceed with the deletion, be aware that all versions of a backup file are deleted from Junos Space Network Management Platform when you initiate a delete operation.

This delete operation does not delete the versions of the backup file from the device.

3. Click **Delete**.

The Delete Configuration Files dialog box appears, announcing that Junos Space Network Management Platform has successfully scheduled the deletion of the selected configuration files. Perform one of the following actions:

- Click the job ID on the Delete Configuration Files dialog box to see whether this delete operation is a success or a failure.
 - Go to step 4 to return to the Config Files Management page.
4. Click **OK** on the Delete Configuration Files dialog box to close the dialog box.

The Config Files Management page reappears, displaying any remaining configuration files.

When you delete a configuration file, an audit log entry is automatically generated. From the audit log entry, you can identify the user who initiated the delete operation, the IP address from which this task was initiated, and so on.

Related Documentation

- [Managing Configuration Files Overview on page 473](#)

- [Restoring Configuration Files on page 478](#)
- [Comparing Configuration Files on page 480](#)
- [Editing Configuration Files on page 482](#)
- [Exporting Configuration Files on page 484](#)

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 file on the device, or overriding the device's running configuration file with a candidate configuration file (a configuration file edited in the Configuration Files workspace) or a configuration backup file from Junos Space Network Management Platform.

When you restore a configuration file, an audit log entry is automatically generated.

To restore a device configuration file from Junos Space Network Management Platform to a device:

1. On the Junos Space Network Management Platform user interface, select **Configuration Files > Config Files Management**.

The Config Files Management page appears.

2. On the Config Files Management page, select the device whose configuration you want to restore. (To restore all of them, select the check box in the column header next to the first column header.)

3. Select **Restore Configuration Files** 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 is merged with the existing configuration on the device. If the filename column is not displayed by default, click the down arrow next to any of the displayed columns and select the **Config File Name** column from the **Columns** list.

4. Select the appropriate version from the drop-down list that appears when you click next to the version number displayed in the **ConfigFile Version** column.

The timestamp is displayed adjacent to the version number. It indicates the time at which this version of the configuration was backed up.

5. Select the appropriate type of restore from the list that appears when you click the term displayed under the **Type** column. You can opt to merge the contents of a configuration file on Junos Space Network Management Platform with the existing configuration file on the device, or override the device's running configuration file with a candidate configuration file (a configuration file edited in the Configuration Files workspace) or a configuration backup file from Junos Space Network Management Platform.

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 is displayed 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 is indicated by the word **Success** in the **Status** column on the **Job Management** page. If a device cannot be accessed, it is skipped over, and the job status indicates a failure.

7. Click **OK** to close the **Restore Configuration Files** dialog box.

Verify your work either by double-clicking the configuration file name on the **Config Files Management** page, or by performing another backup operation and, then comparing versions (see [“Comparing Configuration Files” on page 480](#)).

**Related
Documentation**

- [Managing Configuration Files Overview on page 473](#)
- [Deleting Configuration Files on page 477](#)
- [Comparing Configuration Files on page 480](#)
- [Editing Configuration Files on page 482](#)
- [Exporting Configuration Files on page 484](#)
- [Backing Up Configuration Files on page 488](#)
- [Viewing Audit Logs on page 604](#)

Comparing Configuration Files

View entire device configuration files side by side to compare them, see the total number of diffs, the date and time of the last commit operation, and the number of changes made.

Comparing configuration files does not generate an audit log entry.

You can compare the following:

- The configuration file of one device with 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

To compare device configuration files:

1. On the Junos Space Network Management Platform user interface, 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. On the Config Files Management page, select the configuration file that you want to compare.
3. Select **Compare Configuration File Versions** from the Actions menu.

The Compare Config Files page appears.

4. For the source, select the source device from the **Source Device** list and a version of the configuration file from the **ConfigFile Version** list.

The timestamp is displayed adjacent to the version number. It indicates the time at which this version of the configuration was backed up.

5. For the target, select the target device from the **Target Device** list and a version of the configuration file from the **ConfigFile Version** list.

Timestamp is displayed adjacent to the version number and indicates the time at which this version of the configuration was backed up.

6. Click **Compare**.

The View Diff page appears and 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 that is 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 that is 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 operation 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 long.

7. (Optional) To locate differences in configuration, click **Prev Diff** or **Next Diff**.
8. (Optional) To export differences in the configuration to your local system, click **Export Diff**.

A dialog box appears prompting you to save the zip file.

- a. Save the zip file to your computer. The filename is of the following format:
source-hostname.VersionNumber_target-hostname.VersionNumber.conf
- b. Extract the zip file and open the extracted file by using a browser or a Notepad.

The application lists the differences in the configuration. The first two lines in the extracted file represent the device name, version number, and timestamp of the configuration files that were compared.

When you export the configuration differences, an audit log entry is automatically generated.

9. To finish viewing a comparison, click **Close** at the bottom of the View Diff page. You are returned to the Compare Config Files page.
10. Click **Cancel** to exit the Compare Config Files page.

You are returned to the Config Files Management page.

Related Documentation

- [Backing Up Configuration Files on page 488](#)
- [Managing Configuration Files Overview on page 473](#)
- [Deleting Configuration Files on page 477](#)
- [Restoring Configuration Files on page 478](#)
- [Editing Configuration Files on page 482](#)
- [Exporting Configuration Files on page 484](#)

Editing Configuration Files

The **Modify Configuration File** action enables a very advanced user to edit the configuration file of the selected device via a text editor. However, this action in the Configuration Files workspace has no validation and no sanity check. To obtain those features, use the Device Management > Device Configuration > Modify Configuration action in the Devices workspace.

When you edit a configuration file, an audit log entry is automatically generated (see [“Viewing Audit Logs” on page 604](#)); however, unlike configuration files edited in the Devices workspace, files edited in the Configuration Files workspace are not saved as change requests; instead, they are saved as versions. The audit log entry records the name of the configuration file that was modified.

To edit a configuration file in the Configuration Files workspace:

1. On the Junos Space Network Management Platform user interface, select **Configuration Files > Config Files Management**.

The Config Files Management page appears.

2. On the Config Files Management page, select the device whose configuration you want to edit.

If no configuration files are displayed on the page, back up the device configuration files (see [“Backing Up Configuration Files” on page 488](#)).

3. Click the **Modify Configuration File** icon at the top of the Config Files Management page.

The Edit Config File page appears. It displays the name of the device whose configuration you want to edit, the time at which the file was created, the version of the file with the timestamp (that is, when the configuration snapshot was created), and the contents of the file.

4. From the **Version** list, select a version to use as a baseline. By default, the latest version of the file is displayed.

The timestamp is displayed adjacent to the version number. It indicates the time at which this version of the configuration was backed up.

A version can be either a configuration backup file, or an edited copy of the initial backup file. For more information about versioning, see [“Backing Up Configuration Files” on page 488](#).

The selected version appears in the text editor. Note that there are usually both vertical and horizontal scroll bars, and that a configuration file usually has multiple pages. The status bar at the bottom displays the page that you are on and the total number of pages. It also contains paging controls and a Refresh icon. Use the **Show items** list to manage the number of lines of configuration that is displayed on a single page. By default, 50 lines are displayed. You can choose to display 200, 800, 3200, or 10,000 lines.

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.

5. (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.
6. Enter your changes, using the Copy/Paste function if required.



NOTE: Do not click **Modify** until you have finished editing.

7. (Optional) List the changes you have made (or any other information that you want to add) in the **Comments** field. You cannot add a comment unless you have made changes to the configuration. It is advisable to enter text in this field to distinguish the current version from a backup taken from the device itself.
8. After you have made all changes, click **Modify**.

The Config Files Management page reappears, displaying the edited configuration file that is still selected.



NOTE: Junos Space does not create a new version of the configuration file if you have not made any changes to the device configuration. That is, if you click **Modify** without making any changes to the device configuration, then Junos Space displays the following message:
Config file contents are same as the current version. To save as a latest version, please change the contents or select a previous version to be saved as the latest.

Verify your work by double-clicking the device on the Config Files Management page.

A dialog box appears, displaying the file in noneditable format. You can select the version from the **Version** list. By default, the latest edited version appears.

The pagination, Comments area, and controls are the same as they are in the text editor you used to make your changes.

If you want, you can compare versions of the file to view the differences between the recently modified version and a previous version (see [“Comparing Configuration Files” on page 480](#)).

To deploy the edited configuration file on to a device, you must use the Restore action (see [“Restoring Configuration Files” on page 478](#)).

Related Documentation

- [Managing Configuration Files Overview on page 473](#)
- [Deleting Configuration Files on page 477](#)
- [Exporting Configuration Files on page 484](#)
- [Backing Up Configuration Files on page 488](#)

- [Viewing Audit Logs on page 604](#)

Exporting Configuration Files

The Export action enables you to save one or more configuration files to a zip folder on your local computer. You can later view or compare the downloaded configuration files offline.



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 is aborted and the zip folder removed.

When you export a configuration file, an audit log entry is automatically generated.

To export a configuration file to a zip folder on your local computer:

1. On the Junos Space Network Management Platform user interface, select **Configuration Files > Config Files Management**.

The Config Files Management page appears.

2. On the Config Files Management page, select one or more configuration files.



NOTE: If the filename column is not displayed by default, click the down arrow next to any of the displayed columns and select the Config File Name column from the Columns list.

3. Select **Export Config Files** 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.



NOTE: If the filename column is not displayed by default, click the down arrow next to any of the displayed columns and select the Config File Name column from the Columns list.

4. Select the appropriate version from the list that appears when you click next to the version number displayed in the **ConfigFile Version** column.

The timestamp is displayed adjacent to the version number and indicates the time at which this version of the configuration was backed up.

5. Click **Export** on the Export Config File(s) dialog box.

The Generating ZIP archive dialog box appears, displaying a progress bar showing when the zip file is ready for downloading. At this point, the Opening deviceConfigFiles.zip dialog box opens.

6. Save the zip file to your computer before closing the progress bar or the Opening deviceConfigFiles.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 boxes is closed. Refreshing or exiting the browser also removes the zip file from the server.

To view the contents of the device configuration file that you have just exported, extract the zip file and open the extracted file by using a text editor, such as Notepad. If you have exported the configuration file of more than one device, the extracted folder contains one configuration file for each device. The filename of the exported configuration file adheres to the following syntax: *device-name/IP address_version-number_timestamp in YYYYMMDD-hhmmss format-locale.conf*. For example, Device1_3_20131104-082846-IST.conf, where Device1 is the device name, 3 is the version number of the configuration file that was exported, 20131104-082846 is the timestamp when the backup was taken in 24-hour format, and IST represents the time zone.

**Related
Documentation**

- [Managing Configuration Files Overview on page 473](#)
- [Deleting Configuration Files on page 477](#)
- [Restoring Configuration Files on page 478](#)
- [Comparing Configuration Files on page 480](#)
- [Editing Configuration Files on page 482](#)
- [Backing Up Configuration Files on page 488](#)
- [Viewing Audit Logs on page 604](#)

CHAPTER 52

Backup Config Files

- [Backing Up Configuration Files on page 488](#)

Backing Up Configuration Files

Backing up a configuration file in the Configuration Files workspace means importing the configuration file from a device and storing it in Junos Space Network Management Platform.

Backing up your device configuration files is therefore a prerequisite for configuration file management (see [“Managing Configuration Files Overview” on page 473](#)).

Only devices that have been previously discovered can have their configuration files backed up. The backup function skips over any devices that cannot be accessed. On the Job Management page, under State, a skipped-over configuration backup file shows up as Failed.

The backup function checks for differences between the configuration file on the device and the configuration backup file stored in Junos Space Network Management Platform before creating a new version of the configuration file. If no changes are detected, the device is skipped over. However, status is shown as Success on the Job Management page for this backup configuration job.



NOTE: The backup function checks for differences between the configuration file on the device and the configuration backup file 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 back up the file, a new version is created. The first backup file is Version 1, the edited configuration file is Version 2, and the second backup file is Version 3.

When you back a configuration file, an audit log entry is automatically generated. From the audit log entry, you can identify the user who initiated the backup operation, the IP address from which this task was initiated, and so on.



NOTE: In the case of an SRX Series device with LSYS, configuration file backup is supported only on the root device.

To back up configuration files from one or more devices to Junos Space Network Management Platform:

1. On the Junos Space Network Management Platform user interface, select **Configuration Files > Config Files Management**.

The Config Files Management page appears.

2. Click the **Backup Configuration Files** icon.

The Backup Configuration 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. For more information about tagging, see [“Tagging an Object” on page 793](#).

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.

3. Select the devices from the table whose configurations you want to back up by using either of the following selection modes—manually or on the basis of tags. These options are mutually exclusive. If you select one, the other is disabled.



NOTE: By default the **Select by Device** option button is selected and the complete list of devices is displayed.

To select devices manually:

- a. Click the **Select by Device** option and select the devices 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 the **Host Name** column.

To select devices on the basis of 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, displaying two categories of tags—Public and Private.
- c. 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.

To search for a specific tag, enter the first few letters of the tag name 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.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

4. (Optional) 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.

If you do not select the **Schedule at a Later Time** check box, the configuration files are backed up as soon as you click the **Backup** button on the Backup Config Files page.

5. (Optional) Schedule configuration files backup recurrence by selecting **Repeat**.

- a. Specify the backup recurrence by setting the interval and the increment.

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 backup operation will recur endlessly until you cancel the job manually.

6. Click **Backup** at the bottom of the Backup Configuration Files page.

The Backup Configuration Files dialog box appears, announcing that Junos Space Network Management Platform has successfully scheduled backup of the selected configuration files. Click the job ID on the Backup Configuration Files dialog box to see whether this job is a success or a failure. Otherwise, go to step 7 to return to the Config Files Management page to view the configuration files managed by the Junos Space server.



NOTE: The job of backing up a configuration file may fail. To find out why the backup job failed:

- a. From the Job Management page, double-click the row that contains the backup job.

The Configuration File Management Job Status page appears.

- b. From the Status column on the Configuration File Management Job Status page, locate the job that has failed.

- c. For the failed job, click View Results in the Description column.

The Job Description page displays the reason for failure—for example, the device was down at the time of the backup operation.



NOTE: If the device configuration stored on the device and the Junos Space server are the same, then Junos Space displays the following message on the Job Description page: **Config file contents from the device are same as the latest version of the Config file present in JUNOS Space. File not backed up.**

- d. Click Close at the bottom of the Job Description page. You are returned to the Configuration File Management Job Status page.

- e. Click the [X] icon at the top left of the Configuration File Management Job Status page to return to the Job Management page.

7. Click OK on the Backup Configuration Files dialog box to close the dialog box.

The Config Files Management page reappears, displaying the backup files. This page displays the following information:

- **Config File Name**—Device serial name with the .conf file extension.
- **Device Name**—Name of the device whose configuration file is backed up
- **Latest ConfigFile Version**—Latest version number of the backup configuration file
- **Creation Date**—Timestamp when version 1 of the configuration file is created on the Junos Space server. It corresponds to the time at which you back up a device configuration for the first time from the Junos Space server.

When you migrate from a previous release of Junos Space Network Management Platform to the current release, the creation date that is displayed for the various versions of the configuration files of the previous release is as follows:

- For version 1, the creation date is the time at which this file was created in the previous release. For example, if you had backed up a device configuration on Dec 9, 2012 12:51:06 PM IST in Junos Space Release 13.1 and migrated to Junos Space Release 13.3R1 in 2014, the creation date of this file is displayed as Dec 9, 2012 12:51:06 PM IST instead of a date in 2014.

- For all versions greater than one, the creation date is the time at which these versions were created in the previous release. For example, consider that you modified version 1 of the configuration file to version 2 on Dec 15 2012 7:28:46 PM IST in Junos Space Release 13.1 and migrated to Junos Space Release 13.3R1 in 2014, the creation date for version 2 is displayed as Dec 15 2012 7:28:46 PM IST instead of a date in 2014.

- **Last Updated Date**—Timestamp when the device configuration was last modified.

When you modify the device configuration, this action results in the addition of a newer version of the configuration file. Therefore, this timestamp corresponds to the time at which the latest version of the configuration file is created on the Junos Space server.

Click any column header to reveal the down arrow, which you can click to sort, add, or delete columns. You can also filter the data that is displayed on all the columns except Creation Date and Last Updated Date columns. For instructions on filtering, see “Filter Submenus” in *Inventory Landing Page*.

For troubleshooting, see the `/var/log/jboss/server.log` file.

Related Documentation

- [Managing Configuration Files Overview on page 473](#)
- [Deleting Configuration Files on page 477](#)
- [Restoring Configuration Files on page 478](#)
- [Comparing Configuration Files on page 480](#)
- [Editing Configuration Files on page 482](#)
- [Exporting Configuration Files on page 484](#)
- [Tagging an Object on page 793](#)
- [Viewing Audit Logs on page 604](#)

PART 9

Jobs

- [Overview on page 495](#)
- [Manage Jobs on page 499](#)
- [Archive Jobs on page 513](#)

Overview

- [Jobs Overview on page 495](#)

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 any object that is managed by Junos Space, such as a device, service, or customer. All scheduled jobs can be monitored.

Typical jobs in Junos Space Network Management Platform include discovering devices, 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) on the Job Management 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 66: 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 500](#)
- [Viewing Statistics for Scheduled Jobs on page 503](#)
- [Viewing Objects on Which a Job is Executed on page 504](#)
- [Reassigning Jobs on page 506](#)
- [Canceling a Job on page 509](#)
- [Viewing Database Backup Job Recurrence on page 510](#)
- [Archiving and Purging Jobs on page 513](#)

CHAPTER 54

Manage Jobs

- [Viewing Your Jobs on page 499](#)
- [Viewing Scheduled Jobs on page 500](#)
- [Viewing Statistics for Scheduled Jobs on page 503](#)
- [Viewing Objects on Which a Job is Executed on page 504](#)
- [Reassigning Jobs on page 506](#)
- [Canceling a Job on page 509](#)
- [Deleting Your Jobs on page 510](#)
- [Viewing Database Backup Job Recurrence on page 510](#)
- [Retrying a Job on Failed Devices on page 511](#)

Viewing Your Jobs

You can view all your completed, in-progress, canceled, 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 (see [“Deleting Your Jobs” on page 510](#)).

To view the jobs that you have initiated:

1. In the banner of the Junos Space user interface, click the **My Jobs** icon located at the top right.

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 appears and displays a list 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. Click **Close** to exit the My Jobs page.

For troubleshooting, see the `/var/log/jboss/server.log` file.

Related Documentation

- [Viewing Statistics for Scheduled Jobs on page 503](#)
- [Canceling a Job on page 509](#)
- [Jobs Overview on page 495](#)

Viewing Scheduled Jobs

The Job Management inventory page displays all jobs that have been scheduled to run or have run from each Junos Space application.

- [View on page 500](#)
- [Viewing Job Types on page 500](#)
- [Viewing Job Status Indicators on page 500](#)
- [Viewing Job Details, Status, and Results on page 501](#)
- [Executing Commands on Jobs on page 502](#)

View

Scheduled and completed jobs appear as rows in the Jobs inventory table. By default, jobs appear sorted by scheduled start time. You can sort on other criteria as well.

To display the Jobs table:

- On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.
The Job Management page appears and displays the jobs in tabular view.

Viewing Job Types

The job type appears as a column in the Jobs table. Job types indicate what tasks or operations have been performed across 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* in the *Junos Space User Interface Guide*.

Viewing Job Status Indicators

Each job has a job status indicator. [Table 67 on page 500](#) defines these indicators.

Table 67: Job Icon Status Indicators






Job Status Indicator	Description
	The job was completed successfully.

Table 67: Job Icon Status Indicators (*continued*)

	The job failed.
	The job was canceled by a user.
	The job is scheduled.
	The job is in progress. You can cancel only those jobs that are in progress from the Actions menu.

Viewing Job Details, Status, and Results

The Jobs table shows most of what you need to know about each job. You can obtain more details about a particular job from the Job Details page. To see these details, double-click that job's row in the Jobs table.

[Table 68 on page 501](#) defines job information. The job information that appears in the Jobs table and on the View Job Details page varies with the type of job. This table defines all the possible entries.

Table 68: Job Details and Columns in the Jobs Table

Field	Description
Job Type	Supported job types. The Junos Space applications determine which job types are supported.
ID	ID of the job
Domain	Domain from which the job is initiated
Name	Name of the job. 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	Percentage of the job that is 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.
Parameters	Objects on which a job is performed or is scheduled to be performed
Scheduled Start Time	Start time that you specified for this job
Owner	User's login name

Table 68: Job Details and Columns in the Jobs Table (*continued*)

Summary	Operations executed for the job
Recurrence	Scheduled recurrence
Retry Group ID	Job ID of the original job
Previous Retry	Job ID of the previous job
Job Details (depending on job type):	
IP Address	Address of the device on which the operation is performed
Hostname	Name of the device on which the operation is performed
Status	Job status: SUCCESS, Failed, IN PROGRESS, or CANCELED.
Description	Details about a failure
Actual Start Time	Time when Junos Space Network Management Platform begins to execute the job. In most cases, the actual start time should be the same as the scheduled start time.
End Time	Time when the job was completed or was terminated, if job execution failed

Executing Commands on Jobs

You can execute the following commands from the Jobs Actions menu:

- **Cancel Job**—Stops a scheduled job. See [“Canceling a Job” on page 509](#).
- **Reassign Jobs**—Reassigns scheduled or recurring jobs of a user to another user. See [“Reassigning Jobs” on page 506](#).
- **Retry on Failed Devices**—Retries a failed job on the devices. See [“Retrying a Job on Failed Devices” on page 511](#).
- **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 510](#).
- **Return to Application**—Returns to the application page from which this job was initiated (if you have the correct permissions to do so). For example, if you selected a database backup recurrence job, then click **Return to Application** to go to the Database Backup and Restore page.
- **Tag It**—Applies a tag to a job to segregate, filter, and categorize jobs. See [“Tagging an Object” on page 793](#).
- **View Tags**—Displays tags applied to a job. See [“Viewing Tags for a Managed Object” on page 794](#).
- **UnTag It**—Removes a tag from a job. See [“Untagging Objects” on page 794](#).

- Related Documentation**
- [Viewing Statistics for Scheduled Jobs on page 503](#)
 - [Jobs Overview on page 495](#)
 - [Canceling a Job on page 509](#)

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 503](#)
- [Viewing the State of Jobs That Have Run on page 503](#)
- [Viewing Average Execution Times for Jobs on page 504](#)

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 that is displayed on the right identifies the job type titles using colors. Scroll down the list to see all job types. Mouse over a slice in the pie chart to view the job type title and the number of jobs that are 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 500](#).
- To return to the Job Management page, select **Job Management** from the breadcrumbs at the top of the Jobs page.

Viewing the State of Jobs That Have Run

The State of Jobs Run pie chart graphically displays the percentages of jobs that succeeded, are canceled, are in-progress, or failed. Mouse over the pie chart to see the state and percentage of jobs run in each slice.

- To display details of only those jobs that succeeded, those that were cancelled, or those that failed, click the appropriate slice in the State of Jobs Run pie chart.
The filtered jobs are displayed in tabular form on the Job Management page. For more information about the Job Management page, see [“Viewing Scheduled Jobs” on page 500](#).
- To return to the Jobs page, select **Jobs** from the breadcrumbs at the top of the 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 are displayed in tabular form on the Job Management page. For more information about the Job Management page, see [“Viewing Scheduled Jobs” on page 500](#).
- To return to the Jobs page, select **Jobs** from the breadcrumbs at the top of the page.

Related Documentation

- [Viewing Scheduled Jobs on page 500](#)
- [Jobs Overview on page 495](#)
- [Archiving and Purging Jobs on page 513](#)

Viewing Objects on Which a Job is Executed

A job is a user-initiated action that is executed on any object that is managed by Junos Space, such as a device, service, or customer. From the Job Management inventory page, you can view the objects on which a job was performed or is scheduled to be performed. The **Parameters** column on this page provides you with this information. However, for jobs that are migrated from releases prior to Junos Space 13.3R1, this column does not display any information (that is, it is empty).

When you archive jobs, the data in the **Parameters** column is also archived along with other information.

To view objects on which a job is executed:

1. On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.

The Job Management page displays the jobs in tabular view.

2. Select a job.

The **Parameters** column for the selected job provides information about objects on which the job is performed.

For example, when you select a Stage Scripts job, this column displays the device name and the script name associated with this job if you staged a single script on a single device. If you staged multiple scripts on multiple devices, then this column displays the count of the scripts and the number of devices on which these scripts were staged.

3. Click the link in the **Parameters** column to view information about the objects.

The View Job Parameters dialog box appears, displaying the parameter types in separate tabs.

4. Click the tab that you are interested in to view the objects.

If you staged multiple scripts on multiple devices, click the **Device(s)** tab to view the list of devices on the which the scripts were staged. Click the **Script(s)** tab to view the scripts that were staged on these devices.



NOTE: It is not always necessary that the list of devices be displayed on the Device(s) tab. Script and image jobs may display the tag names or CSV filenames instead of devices. For example, if you used a CSV file for staging or deploying an image, the filename of this CSV file is displayed instead of the devices on which the image is staged or deployed. This logic applies to tag names as well.

5. Click **OK** on the View Job Parameters dialog box to return to the Job Management page.

Table 69: Jobs that Support Viewing Objects on Which a Job is Executed

Workspace	Jobs
Device Management	Upload keys to devices
	Modify authentication
	Discover devices
	Resynchronize devices
CLI Configlets	Apply CLI configlet

Table 69: Jobs that Support Viewing Objects on Which a Job is Executed (*continued*)

Workspace	Jobs
Images and Scripts	<p>Images</p> <ul style="list-style-type: none"> • Stage an image on a device • Verify checksum • Deploy a device image <hr/> <p>Scripts:</p> <ul style="list-style-type: none"> • Stage a script on devices • Verify a script on devices • Disable scripts on devices • Enable scripts on devices • Execute a script on devices • Remove a script from devices <hr/> <p>Operations:</p> <ul style="list-style-type: none"> • Run operations <hr/> <p>Script bundles:</p> <ul style="list-style-type: none"> • Stage a script bundle on devices • Execute a script bundle on devices • Disable a script bundle on devices • Enable a script bundle on devices

Related Documentation

- [Jobs Overview on page 495](#)

Reassigning Jobs

You can reassign jobs owned by a user to another user within the same domain from the Job Management workspace by using the **Reassign Jobs** task. When you reassign jobs, you are transferring the ownership of these jobs from one user to another. For example, if you delete UserA, you might want to reassign the jobs of UserA to UserB to ensure that the scheduled and recurring jobs of UserA are monitored and taken to successful completion by UserB.

If you are a user who is assigned the privileges of a Job Administrator, you can reassign jobs scheduled by any user. If you are a user who is assigned the privileges of a Job User, you cannot reassign jobs to other users. If you are assigned a role that does not allow you to reassign any job, you cannot reassign 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.

To reassign a job:

1. On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.

The Job Management inventory page appears.

2. Select the jobs that you want to reassign.



TIP: A quick way to reassign scheduled and recurring jobs of UserA to UserB is to perform the following steps:

- a. Click the down arrow next to the **Owner** column header.
- b. Mouse over **Filters** and type the filter criteria in the text box.
In this example, type UserA.

- c. Click **Go**.

The Job Management displays all jobs owned by UserA.

- d. Click the down arrow next to the **State** column header.
- e. Mouse over **Filters** and type the filter criteria in the text box.
In this example, select SCHEDULED and RECURRING.

- f. Click **Go**.

The Job Management page displays all scheduled and recurring jobs owned by UserA.

You can filter data in other columns where filtering is supported. Follow the same procedure to filter data in columns that are of interest to you.

3. Select **Reassign Jobs** from the Actions menu.

The Reassign Jobs dialog box appears, displaying the active users who are in the same domain as the user whose jobs you want to reassign. This dialog box does not display disabled users.

If **Reassign Jobs** is disabled, it means that one or more jobs that you selected are completed, in progress, or canceled. Go to step 2 and select only scheduled and recurring jobs.

4. Use the vertical scroll bar to navigate to the user to whom you want to reassign the jobs.

You can also filter, or sort the users in ascending or descending order, to quickly locate the user to whom you want to reassign the jobs.

5. Select the user.
6. Click **Reassign**.

The selected jobs are reassigned to the new user and an information dialog box appears confirming the successful reassignment. However, if the assigned user does not have access to the workspaces to which the jobs belong, then any retry or recurrence of the jobs fail and the jobs are canceled. The jobs stay in this state until there is administrator intervention. The following jobs support this behavior:

- Resynchronize network elements.
 - Execute a script bundle.
 - Enable a script bundle.
 - Disable a script bundle.
 - Stage a script bundle.
 - Verify a device image.
 - Delete a device image from the staged devices.
 - Remove an image from device.
 - Stage a device image.
 - Deploy a device image.
 - Deploy a template.
 - Edit device configuration.
 - Validate device configuration.
 - Deploy device configuration.
 - Back up the database.
7. Click **OK** on the information dialog box to return to the Job Management page.

The **Owner** column on Job Management page now displays the new owner of the reassigned jobs.

When the new owner clicks the **My Jobs** icon at the top of the Junos Space user interface, the owner can see these reassigned jobs in the My Jobs report. The old owners cannot view the reassigned jobs in their My Job reports.

When you reassign a job, an audit log entry is automatically generated and details about the reassigned job are recorded.

To obtain details about jobs that were reassigned from an audit log entry:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs > Audit Log**.

The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using the **Reassign Jobs** keyword.

Then the Audit Log page displays only the audit log entries that were generated when the jobs were reassigned.

3. Double-click an audit log entry.

The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of jobs that were reassigned and the **Affected Object Detail** section displays details about each job and the owner to which it is reassigned.

4. Click **OK** on the Audit Log Detail page to exit this page.

You are returned to the Audit Log page.

Related Documentation

- [Jobs Overview on page 495](#)

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 cancel only those 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 clean up canceled jobs.

All jobs except the jobs you triggered are disabled.

To cancel a job:

1. On the Junos Space Network Management Platform user interface, 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 on 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 503](#)
 - [Jobs Overview on page 495](#)
 - [Viewing Scheduled Jobs on page 500](#)
 - [Viewing Your Jobs on page 499](#)

Deleting Your Jobs

You can clear your jobs from a list of your jobs when these jobs are no longer of interest to you.

To remove the jobs that you have initiated:

1. In the banner of the Junos Space user interface, click the **My Jobs** icon located at the top right.

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. Perform one of the following actions:
 - Click the **Clear Job** icon that appears to the right of the job to remove a job.
 - Click **Clear All My Jobs** at the top of the My Jobs report to clear all your jobs displayed on the My Jobs list.



NOTE: Clearing a job from the My Jobs report does not affect the job itself, but only updates the My Jobs view.

3. Click **Close** to exit the My Jobs page.

- Related Documentation**
- [Viewing Your Jobs on page 499](#)
 - [Jobs Overview on page 495](#)

Viewing Database Backup 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. On the Junos Space Network Management Platform user interface, 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 686](#)
- [Viewing Scheduled Jobs on page 500](#)
- [Viewing Audit Logs on page 604](#)

Retrying a Job on Failed Devices

A job could fail for various reasons. To know why the job failed, double-click the failed job. The resultant page displays the reason for failure. You can retry the failed job by performing the following steps.

To retry a job that was not successful:

1. On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.

The Job Management page appears.

2. Select the failed job that you want to retry.
3. From the Actions menu, select **Retry on Failed Devices**.

The Retry Job - Devices Selection page appears.

4. To select the devices on which to run the job, perform one of the following steps:
 - Select devices from the Select Applicable Devices table, showing the following for each device:
 - **Name**—Name of the device
 - **IP Address**—IP address of the device

- **Job Status**—Status of the job: Failed/Failure, Success, or Canceled
- **Description**—Explains the nature of the failure
- Select **Select All Devices Across Pages** to run the job on all devices listed over multiple pages.

The check boxes in the table showing the device listings are unavailable.

5. (Optional) To view the devices on which the job cannot be retried, click **View Inapplicable Devices**.

The View Inapplicable Devices page appears with a table listing all the inapplicable devices. You can view the same information for each device in the Select Applicable Devices table.

To close the View Inapplicable Devices page, click the **x** icon. You are returned to the Retry Job - Devices Selection page.

6. (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 the job from the date and time drop-down lists that appear.

7. Click **Run**.

The Resynchronization Information dialog box appears.

8. Perform one of the following actions on the Resynchronization Information dialog box:
 - To view details about the job that was retried, click the job ID on this dialog box. The Job Management page reappears, displaying the job that you have retried.
 - If you want to close this dialog box, click **OK**.

**Related
Documentation**

- [Jobs Overview on page 495](#)
- [Viewing Your Jobs on page 499](#)

CHAPTER 55

Archive Jobs

- [Archiving and Purging Jobs on page 513](#)

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 reminds you from time to time 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 `yyyy-mm-dd` format; *time* specifies hours, minutes, and seconds, in the `hh-mm-ss` format; and *id* is a six-character number in the `xx-xx-xx` format that uniquely identifies each job archive file.

This topic includes the following tasks:

- [Archiving Jobs to a Local Server and Purging the Jobs from the Database on page 513](#)
- [Archiving Jobs to a Remote Server and Purging the Jobs from the Database on page 514](#)

Archiving Jobs to a Local Server and Purging the Jobs from 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. On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.

The Job Management page appears.

2. Click the **Archive/Purge Jobs** icon. The Archive/Purge Jobs dialog box appears.

3. For 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.

4. For the **Archive Mode** field, select **local** from the list.
5. 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 the Junos Space server time but uses the local time zone of the client computer.

6. Click **Submit**.

The Jobs Archive and Purge Job Information confirmation page appears.
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 Jobs from the Database

You can archive jobs to remote network hosts or media. Junos Space Network Management Platform uses secure copy (scp) 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. On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.

The Job Management page appears.
2. Click the **Archive/Purge Jobs** icon. The Archive/Purge Jobs dialog box appears.
3. For 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.

4. For the **Archive Mode** field, select **remote** from the list (the default).
5. In the **User** field, enter a valid username to access the remote host server.
6. In the **Password** field, enter a valid password to access the remote host server.
7. In the **Confirm Password** field, reenter the password you entered in the previous step.
8. In the **Machine IP** field, enter the IP address of the remote host server.
9. In the **Directory** field, enter a directory path on the remote host server for the archived files.



NOTE: The directory path must already exist on the remote host server. Also, if there is no sufficient space, then Junos Space throws the following message:

Error: Not enough disk space.

10. 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 the Junos Space server time but uses the local time zone of the client computer.

11. Click **Submit**.
The Jobs Archive and Purge dialog box displays the file location and the name of the remote server.
12. Click **Continue** on the Jobs Archive and Purge dialog box to archive and purge the audit logs.
Junos Space Network Management Platform displays the Jobs Archive and Purge Job Information dialog box.
13. Perform one of the following actions:
 - To view job details for the Archive/Purge operation, click the **Job ID** link on the Jobs Archive and Purge Job Information dialog box.
 - Click **OK** to close the Jobs Archive and Purge Job Information dialog box.

**Related
Documentation**

- [Jobs Overview on page 495](#)
- [Viewing Your Jobs on page 499](#)
- [Viewing Scheduled Jobs on page 500](#)
- [Viewing Database Backup Job Recurrence on page 510](#)

PART 10

Users

- [Manage Roles on page 519](#)
- [Manage User-Defined Roles on page 553](#)
- [Manage Domains on page 557](#)
- [Manage Users on page 571](#)
- [Manage Remote Profiles on page 597](#)
- [User Sessions on page 599](#)

CHAPTER 56

Manage Roles

- [Role-Based Access Control Overview on page 519](#)
- [Configuring Users to Manage Objects in Junos Space Overview on page 521](#)
- [Predefined Roles Overview on page 521](#)
- [Managing Roles Overview on page 550](#)
- [Managing Roles on page 551](#)

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 764](#).

Junos Space Network Management Platform also supports certificate-based authentication of a user. Instead of authenticating a user based on the user's credentials, you can authenticate a user based on the user's certificate, which is considered more secure. For more information on certificate-based authentication, see [“Certificate Management Overview” on page 745](#).

RBAC Enforcement

With role-based access control (RBAC) enforcement, a Junos Space Super Administrator or User Administrator controls the workspaces users can access, the system resources users can view and manage, and the tasks available to users within a workspace. RBAC is enforced in the Junos Space user interface navigation hierarchy by workspace, task group, and task. A user can access only those portions of the navigation hierarchy that are explicitly granted through access privileges. 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 on 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 521](#)
- [Predefined Roles Overview on page 521](#)
- [Creating User Accounts on page 571](#)
- [Viewing User Statistics on page 595](#)
- [Viewing Users on page 582](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 764](#)

Configuring Users to Manage Objects in Junos Space Overview

Junos Space Network Management Platform is shipped with a Super Administrator privilege level that provides full access to the Junos Space system. When you first log in to Junos Space Network Management Platform as default Super Administrator, you can perform all tasks and access all Junos Space system resources. 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 about the predefined roles, see [“Predefined Roles Overview” on page 521](#).

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.



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 519](#)
- [Creating User Accounts on page 571](#)
- [Viewing Users on page 582](#)
- [Viewing User Statistics on page 595](#)

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 70 on page 522 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 > Role Based Access Control > Roles**.

Table 70: 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 Log <ul style="list-style-type: none"> Archive/Purge Logs Export Audit Logs 	Network Management Platform > Audit Logs
CLI Configlets Manager	<ul style="list-style-type: none"> CLI Configlets <ul style="list-style-type: none"> Configlets <ul style="list-style-type: none"> Create CLI Configlet Delete CLI Configlets Compare CLI Configlet Versions View CLI Configlet Details Modify CLI Configlet Clone CLI Configlet Apply CLI Configlet Export Selected CLI Configlets Export All CLI Configlets Import CLI Configlet Assign Cli Template to Domain 	Network Management Platform > CLI Configlets
	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Management <ul style="list-style-type: none"> Apply CLI Configlet Secure Console 	Network Management Platform > Devices

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
CLI Configlets Operator	<ul style="list-style-type: none"> CLI Configlets <ul style="list-style-type: none"> Configlets Apply CLI Configlet 	Network Management Platform > CLI Configlets
	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Management Secure Console 	Network Management Platform > Devices
Configuration File Manager	<ul style="list-style-type: none"> Configuration Files <ul style="list-style-type: none"> Config Files Management <ul style="list-style-type: none"> Backup Configuration Files Delete Configuration Files Restore Configuration Files Compare Config File Versions Export Configuration File Modify Configuration File 	Network Management Platform > Configuration Files
Configuration View Manager	<ul style="list-style-type: none"> CLI Configlets <ul style="list-style-type: none"> Configuration View <ul style="list-style-type: none"> Create Configuration View Modify Configuration View Delete Configuration View View Configuration View Details 	Network Management Platform > CLI Configlets
	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Management <ul style="list-style-type: none"> Device Configuration <ul style="list-style-type: none"> View Active Configuration Secure Console 	Network Management Platform > Devices

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Configuration View Operator	<ul style="list-style-type: none"> CLI Configlets <ul style="list-style-type: none"> Configuration View 	Network Management Platform > CLI Configlets
	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Management <ul style="list-style-type: none"> Device Configuration <ul style="list-style-type: none"> View Active Configuration Secure Console 	Network Management Platform > Devices
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 	Network Management Platform > Devices
	<ul style="list-style-type: none"> Images and Scripts <ul style="list-style-type: none"> Images <ul style="list-style-type: none"> Import Images View Deployed Results Modify Device Image Delete Device Images Stage Image on Device MD5 Validation Result Verify Image on Devices Deploy Device Image Remove Image from Staged Device View Associated Devices Assign Image to Domain 	Network Management Platform > Images and Scripts
Device Images Read Only User	<ul style="list-style-type: none"> Images and Scripts <ul style="list-style-type: none"> Images <ul style="list-style-type: none"> View Deployed Results View Associated Devices 	Network Management Platform > Images and Scripts

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace	
Device Manager		Network Management Platform > Devices	

Table 70: 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 Management <ul style="list-style-type: none"> • Device Configuration <ul style="list-style-type: none"> • View Active Configuration <ul style="list-style-type: none"> • Create/Edit/Delete Filter • Resolve Out-of-band Changes • View/Assign Shared Objects • View Configuration Change Log • View Template Deployment • Modify Unmanaged Device Configuration • Review/Deploy Configuration <ul style="list-style-type: none"> • Validate on Device • Approve • Reject • Deploy • Modify Configuration • Assign Device to Domain • Device Inventory <ul style="list-style-type: none"> • Export Physical Inventory • View Associate Scripts • View License Inventory • View Logical Interfaces • View Physical Interfaces • View Physical Inventory • View Script Executions • View Inventory Changes • View Software Inventory • View Staged Images <ul style="list-style-type: none"> • Delete Staged 	

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> Images <ul style="list-style-type: none"> Verify Checksum Device Operations <ul style="list-style-type: none"> Create LSYS Manage Device Partition <ul style="list-style-type: none"> Create Partition Modify Partition Delete Partition Assign Partition to Domain Delete Devices Looking Glass Put in RMA State Reactivate from RMA Resynchronize with Network Execute Scripts Apply CLI Configlet Reboot Devices Device Access <ul style="list-style-type: none"> Modify Authentication Launch Device WebUI SSH to Device Resolve Key Conflict Manage Customized Attributes <ul style="list-style-type: none"> Add Label Delete Label Upload Keys to Devices Modify Serial Number Secure Console Modify Device Configuration Device Discovery <ul style="list-style-type: none"> Discover Targets Specify Probes Specify Credentials 	

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> Model Devices <ul style="list-style-type: none"> Create Modeled Instance Add More Devices View Modeled Instance View Modeled Device Status View Configlet Download Configlet Delete Modeled Instances Connection Profiles <ul style="list-style-type: none"> Create Connection Profile Modify Connection Profile View Connection Profile Delete Connection Profiles Clone Connection Profile Unmanaged Devices View Alarms View Performance Graphs 	

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Script Manager	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> View Script Executions 	Network Management Platform > Devices
	<ul style="list-style-type: none"> Images and Scripts <ul style="list-style-type: none"> Scripts <ul style="list-style-type: none"> Compare Script Versions Import Script View Execution Results Modify Script Modify And Stage Scripts on Device 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 Assign Script to Domain Script Bundles <ul style="list-style-type: none"> Create Script Bundle Embedded Script Modify Script Bundle Delete Script Bundles Stage Script Bundle on Devices View Associated Devices Enable Script Bundle on Devices Disable Script Bundle on Devices Execute Script Bundle on Devices 	Network Management Platform > Images and Scripts

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Script Operator	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Management Secure Console 	Network Management Platform > Devices
	<ul style="list-style-type: none"> Images and Scripts <ul style="list-style-type: none"> Scripts <ul style="list-style-type: none"> Compare Script Versions Execute Script on Devices 	Network Management Platform > Images and Scripts
Device Script Read Only User	<ul style="list-style-type: none"> 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
Domain Administrator	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Device Management Secure Console 	Network Management Platform > Devices
	<ul style="list-style-type: none"> Role Based Access Control <ul style="list-style-type: none"> Domains <ul style="list-style-type: none"> Create Domain Modify Domain Delete Domain Assign Devices to Domain Assign Domain to Users User Accounts 	Network Management Platform > Role Based Access Control

Table 70: 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
FMPM Read Only User	<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 	Network Management Platform > Network Monitoring
Job Administrator	<ul style="list-style-type: none"> Jobs <ul style="list-style-type: none"> Job Management <ul style="list-style-type: none"> Cancel My Job <ul style="list-style-type: none"> Cancel Any Job Reassign Jobs Archive/Purge Jobs View Recurrence 	Network Management Platform > Jobs
Job User	<ul style="list-style-type: none"> Jobs <ul style="list-style-type: none"> Job Management <ul style="list-style-type: none"> Cancel My Job View Recurrence 	Network Management Platform > Jobs

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Operation Manager	<ul style="list-style-type: none">Devices<ul style="list-style-type: none">Device Adapter<ul style="list-style-type: none">Add AdapterUpgrade AdapterDelete AdapterView Script Executions	Network Management Platform > Devices
		Network Management Platform > Images and Scripts

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> Images and Scripts <ul style="list-style-type: none"> Images <ul style="list-style-type: none"> Import Images View Deployed Results Modify Device Image Delete Device Images Stage Image on Device MD5 Validation Result Verify Image on Devices Deploy Device Image Remove Image from Staged Device View Associated Devices Assign Image to Domain Scripts <ul style="list-style-type: none"> Compare Script Versions Import Script View Execution Results Modify Script Modify And Stage Scripts on Device 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 Assign Script to Domain Script Bundles 	

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Create Script Bundle • Embedded Script • Modify Script Bundle • View Associated Devices • Enable Script Bundle on Devices • Disable Script Bundle on Devices • Delete Script Bundles • Stage Script Bundle on Devices • Execute Script Bundle on Devices • Assign Script Bundle to Domain • Operations <ul style="list-style-type: none"> • Create Operation • Clone Operation • Copy Operation • Modify Operation • Delete Operations • Import Operations • Export Operations • Run Operation • View Operation Results • Assign Operation to Domain 	
Report Administrator	<ul style="list-style-type: none"> • Reports <ul style="list-style-type: none"> • Generated Reports <ul style="list-style-type: none"> • Delete Generated Report • View Generated Report 	Network Management Platform > Reports

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Report Definition Administrator	<ul style="list-style-type: none"> • Reports <ul style="list-style-type: none"> • Report Definitions <ul style="list-style-type: none"> • Create Report Definition • Modify Report Definition • Delete Report Definition • Clone Report Definition • View Report Definition • Generate Report 	Network Management Platform > Reports
Super Administrator	Manages all Junos Space Network Management Platform task groups and tasks. See Network Management Platform > Users > Roles for a list of tasks that are currently supported.	Access all Junos Space Network Management Platform workspaces.

Table 70: 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 SNMP Manager SNMP Start SNMP Stop SNMP Restart System Snapshot Generate Key Database Backup and Restore <ul style="list-style-type: none"> Database Backup Delete Backup Restore Restore From Remote File Space Troubleshooting Applications <ul style="list-style-type: none"> Modify Application Settings Refresh search index Manage Services Uninstall Application Upgrade Application Add Application Upgrade Platform Licenses <ul style="list-style-type: none"> Import License Tags <ul style="list-style-type: none"> Create Public Tag Modify Public Tag Delete Public Tags Make Tag Public DMI Schemas <ul style="list-style-type: none"> Set Default Schema Report Missing Schemas Update Schema Authentication Servers Platform Certificate CA/CRL Certificates SMTP Servers 	Network Management Platform > Administration

Table 70: 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"> Modify Public Tag Delete Public Tags Make Tag Public Create Public Tag 	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 Assign Definition to Domain 	Network Management Platform > Device Templates > Definitions

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Template Manager	<ul style="list-style-type: none"> • Device Templates <ul style="list-style-type: none"> • Templates <ul style="list-style-type: none"> • Create Quick Template • Create Template • Template Details • Modify Template • Modify Quick Template • Delete Template • Deploy Template • Audit Template Configuration • Undeploy Template • View Template Deployment • Assign Template to Domain • Template Consolidated Configuration • Manage CSV Files 	Network Management Platform > Device Templates > Templates
User Administrator	<ul style="list-style-type: none"> • Role Based Access Control <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 • Unlock Users • Roles <ul style="list-style-type: none"> • Create Role • Modify Role • Delete Roles • 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 > Role Based Access Control

Table 70: Predefined Roles for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Xpath and Regex Manager	<ul style="list-style-type: none"> CLI Configlets <ul style="list-style-type: none"> Xpath and Regex <ul style="list-style-type: none"> Create Xpath / Regex Modify Xpath / Regex Delete Xpath / Regex Assign XPath / Regex to Domain 	Network Management Platform > CLI Configlets

[Table 71 on page 539](#) shows the Junos Space predefined roles for the Network Activate application.

Table 71: Predefined Roles for the 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
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

Table 71: Predefined Roles for the Network Activate Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
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 72 on page 541](#) shows the Junos Space predefined roles for the Service Insight application.

Table 72: Predefined Roles for the Service Insight Application

Predefined Role	Task Group and Tasks
Service Insight Admin	<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 Generate PBN Reports EOL Reports <ul style="list-style-type: none"> Regenerate EOL Reports Export EOL Reports Delete PBN Reports <ul style="list-style-type: none"> Regenerate PBN Reports Export PBN 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 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

Table 72: Predefined Roles for the Service Insight Application (*continued*)

Predefined Role	Task Group and Tasks
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 Generate PBN Reports EOL Reports <ul style="list-style-type: none"> Regenerate EOL Reports Export EOL Reports Delete PBN Reports <ul style="list-style-type: none"> Regenerate PBN Reports Export PBN 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

[Table 73 on page 543](#) shows the Junos Space predefined roles for the Service Now application.

Table 73: Predefined Roles for the Service Now Application

Predefined Role	Task Group and Tasks	Workspace
Service Now Admin		All workspaces

Table 73: Predefined Roles for the 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 Delete Associate Device Groups Export Inventory Information Associate Address Group Add Devices Modify Auto Submit Policy Install Event Profile View Incidents Check FTP Server Uninstall Event Profile Create On-Demand Incident Request RMA Organizations <ul style="list-style-type: none"> Associate Address Group Modify Organization Delete Organizations Check Status View Messages Add Organization Add Member Global Settings <ul style="list-style-type: none"> SNMP Configuration <ul style="list-style-type: none"> Manage SNMP Traps Proxy Server Configuration Core File Upload Configuration Device Groups <ul style="list-style-type: none"> Modify Device Group Set as Default Device Group Delete Device Groups Associate Address Group Create Device Group 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 	

Table 73: Predefined Roles for the Service Now Application *(continued)*

Predefined Role	Task Group and Tasks	Workspace
	<ul style="list-style-type: none">• Set as Default Profile• Push to Devices• Auto Submit Policy• Export Incidents Report• Modify Auto Submit Policy• Delete• Change Status• Create Auto Submit Policy	

Table 73: Predefined Roles for the 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 Update Case 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 73: Predefined Roles for the 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 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 Update Case 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 	Administration Service Central

Table 73: Predefined Roles for the 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 	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 Update Case 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 	Service Central

Table 74 on page 549 shows the Junos Space predefined roles for the Ethernet Design application.

Table 74: Predefined Roles for the 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 519](#)
 - [Configuring Users to Manage Objects in Junos Space Overview on page 521](#)
 - [Managing Roles on page 551](#)
 - [Creating a User-Defined Role on page 553](#)
 - [Modifying User-Defined Roles on page 554](#)
 - [Deleting User-Defined Roles on page 555](#)
 - [Creating User Accounts on page 571](#)
 - [Viewing Users on page 582](#)
 - [Viewing User Statistics on page 595](#)

Managing Roles Overview

Roles define the application workspace tasks a user is assigned by 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 in to 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 571](#) and [“Predefined Roles Overview” on page 521](#). 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 **Role Based Access Control > User Accounts** task allows 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 **Role Based Access Control > Roles** inventory page. See [“Managing Roles” on page 551](#).
- Create user-defined roles from the **Role Based Access Control > Roles > Create Role** task. See [“Creating a User-Defined Role” on page 553](#).
- Modify user-defined roles using **Modify Role** on the **Role Based Access Control > Roles** inventory page. See [“Modifying User-Defined Roles” on page 554](#).
- Delete user-defined roles using **Delete Roles** on the **Role Based Access Control > Roles** inventory page. See [“Deleting User-Defined Roles” on page 555](#).
- Tag predefined and user-defined roles to group them for performing actions simultaneously. Select **Tag It** from the Actions menu on the **Role Based Access Control > Roles** inventory page Actions menu. See [“Tagging an Object” on page 793](#).
- View all tags that exist on roles by selecting **View Tags** from the Actions menu on the **Role Based Access Control > Roles** inventory page. See [“Viewing Tags for a Managed Object” on page 794](#).

Related Documentation

- [Role-Based Access Control Overview on page 519](#)
- [Predefined Roles Overview on page 521](#)
- [Creating User Accounts on page 571](#)
- [Managing Roles on page 551](#)
- [Creating a User-Defined Role on page 553](#)
- [Modifying User-Defined Roles on page 554](#)
- [Deleting User-Defined Roles on page 555](#)

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 **Role Based Access Control > Roles** inventory page allows Super Administrator or 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 on page 551](#)
- [Performing Manage Roles Commands on page 551](#)

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, type (that is, whether the role is a predefined role or a custom role), 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. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

The Roles page appears.

2. Double-click a role.

The Role Detail Summary page appears.

The page displays the workspace and workspace tasks.

3. Click the expander button **+** adjacent to the workspaces to view subtasks.
4. Click **OK** on the Role Detail Summary page to exit this page.

You are returned to the Roles page.

Performing Manage Roles Commands

You can perform a task on predefined and user-defined roles by selecting the task from the Actions menu or the shortcut menu that is displayed when you right-click a role, or by clicking the icons at the top of the Roles page. You can perform the **Modify Role** and **Delete Roles** commands only on read-writeable user-defined roles. You cannot manipulate read-only predefined roles. To perform a command, you must first select the role.

You can perform one or more of the following actions on the roles from the Roles page:

- **View Role Details**—View details about the selected role.
- **Modify Role**—Modify the selected user-defined description, application workspaces, and tasks associated with the workspaces. You cannot modify predefined roles. For more information, see [“Modifying User-Defined Roles” on page 554](#).
- **Delete Roles**—Delete the selected user-defined role. You cannot delete predefined roles. For more information, see [“Deleting User-Defined Roles” on page 555](#).
- **Tag It**—Tag one or more selected inventory objects, see, see [“Tagging an Object” on page 793](#).
- **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 794](#).
- **Untag It**—Untag a tag that is applied to an inventory object. For more information, see [“Untagging Objects” on page 794](#).
- **Delete Private Tags**—Delete tags that you created.
- **Clear All Selections**—Clear any role selections you made on the Roles inventory page.
- **Display Quick View**—Displays or hides a small window summarizing data about the selected object.

Related Documentation

- [Role-Based Access Control Overview on page 519](#)
- [Predefined Roles Overview on page 521](#)
- [Creating User Accounts on page 571](#)
- [Creating a User-Defined Role on page 553](#)
- [Modifying User-Defined Roles on page 554](#)
- [Deleting User-Defined Roles on page 555](#)

Manage User-Defined Roles

- [Creating a User-Defined Role on page 553](#)
- [Modifying User-Defined Roles on page 554](#)
- [Deleting User-Defined Roles on page 555](#)

Creating a User-Defined Role

Junos Space Network Management Platform provides read-only predefined roles—that is, Super Administrator, System Administrator, or User Administrator—that you can use to create users to perform tasks that these roles permit. 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. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

The Roles page appears.

2. 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.

3. In the **Title** text box, type a user-defined role name.

The role title cannot exceed 32 characters. The title can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.). Also, the title cannot start with a space.

4. In the **Description** text box, type a user-defined role description.

The role description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. 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

and collapsible tree of associated tasks appear below the selection ribbon for you to modify specific tasks that you want included in the Task Summary pane.

6. Select the specific tasks that you want for the user-defined role. All application workspace tasks are selected by default 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 all tasks under the task node. 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 set in bold-italic; the second-level workspace tree node is set in bold.

7. Click **Create**.

The user-defined role is created, saved, and appears on 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. Junos Space throws the following error message:

Task tree selection can not be empty.

Creation of a role generates an audit log entry.

Related Documentation

- [Predefined Roles Overview on page 521](#)
- [Managing Roles on page 551](#)
- [Modifying User-Defined Roles on page 554](#)
- [Deleting User-Defined Roles on page 555](#)
- [Creating User Accounts on page 571](#)

Modifying User-Defined Roles

Super Administrator and User Administrator can modify user-defined roles. 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. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > 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. Click the **Modify Role** icon.
4. Modify the part of the user-defined role that you want: description, application workspace, or tasks.

The role description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Click **Modify**.

The modified user-defined role is updated on the Roles inventory page.

Modification of a role generates an audit log entry.

Related Documentation

- [Predefined Roles Overview on page 521](#)
- [Creating User Accounts on page 571](#)
- [Managing Roles on page 551](#)
- [Managing Roles Overview on page 550](#)
- [Creating a User-Defined Role on page 553](#)
- [Deleting User-Defined Roles on page 555](#)

Deleting User-Defined Roles

Super Administrator and User Administrator can delete user-defined roles from the **Roles** inventory page only if they are not assigned to other users. You cannot delete predefined roles.

To delete a user-defined role:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

The Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined roles that you want to delete.
3. Click the **Delete Roles** icon.

The Delete Roles dialog box appears asking you for confirmation.

4. Click **Delete**.

The role is deleted from the Roles inventory page. If the role is assigned to other Junos Space Network Management Platform users, you cannot delete the role. Junos Space throws an error message similar to: **Role "test-role-1" cannot be deleted because it is referenced by users: test-role-user (test role user)**.

Deletion of roles generates an audit log entry.

**Related
Documentation**

- [Predefined Roles Overview on page 521](#)
- [Managing Roles on page 551](#)
- [Creating a User-Defined Role on page 553](#)
- [Managing Roles Overview on page 550](#)
- [Modifying User-Defined Roles on page 554](#)
- [Creating User Accounts on page 571](#)

Manage Domains

- [Managing Domains Overview on page 557](#)
- [Working with Domains on page 564](#)

Managing Domains Overview

A domain is a logical grouping of objects, which can include devices, templates, users, and so on. It represents all or a subset of the physical devices and functionality on your network.

Junos Space contains a default top-level domain called the global domain, which can contain additional domains called subdomains. You can create all your devices and their configurations in the global domain, or you can configure additional subdomains within the global domain.



NOTE: Two levels of hierarchy are supported: global domain and its subdomains. On most inventory landing pages, the Domain column displays the domain to which an object belongs.

You can use multiple domains to separate large, geographically distant systems into smaller, more manageable sections and control administrative access to individual systems. You can assign domain administrators or users to manage devices and objects that are assigned to their domains. You can configure in such a way that a user assigned to one domain need not necessarily have access to objects in another domain. You can even restrict users assigned to a domain from viewing objects that are in the parent domain.

For example, a small organization may have only one domain (the global domain) for their entire network, whereas a large, international organization may have several subdomains within the global domain to represent each of its regional office networks across the world.

The Super Administrator automatically has full permissions for all subdomains, so you do not need to assign new subdomains to Super Administrator. However, to assign a subdomain to another administrator or user, you must first create the user with set permissions to operate within the selected subdomain.

You can create users only when you are in the global domain. However, at the time of creating a user, you can assign the user to any available domains. To create and assign a user to one or more subdomains, see [“Creating User Accounts” on page 571](#). If a user is assigned to the global domain, then the user has implicit access to all subdomains.



NOTE: You create users through the Role Based Access Control workspace, which you can access only from the global domain. This means that you need to be logged in to the global domain to create and assign users to various domains. You cannot access this workspace from a subdomain.

By default, all objects in Junos Space Network Management Platform belong to the global domain. Any Junos Space object other than users can belong to only one subdomain at a time. Assigning an object to more than one subdomain fails. You can only reassign an object from one domain to another.

When you log in to the Junos Space server, you can perform actions only on the objects in the domain to which you are assigned. The domain switcher at the top-right corner of the Junos Space user interface indicates the domain that you are in currently. To access objects in another domain that is also assigned to you, select the domain from the domain switcher. You need not log out and log in again to switch from one domain to another.

By default, on any inventory page, the objects belonging to the domain that you are currently in are displayed along with other objects that are predefined for that workspace (for example, Roles ILP displays all the predefined roles as well as custom roles belonging to the domain in which you are currently operating). However, at the time of creating a domain, an administrator can choose to allow users of this domain to have read-only access to the parent domain. Then you can view the objects that are inherited from the parent domain.

When you are logged in to a specific domain, the objects that you create in the domain are automatically assigned to that domain. If you have read-and-write privileges (based on the roles assigned to you), you can perform read-and-write operations on the objects within the domain. However, if you have only read-only permissions, write operations fail. Similarly, if you have read-only access to objects in the parent domain, write operations fail even if you have read-and-write privileges on these objects by virtue of the roles assigned to you (that is, you can only view these objects). If the administrator has not provided you with read-only access to objects in the parent domain, then these objects are not visible to you in the subdomain.

If you are logged in to the parent domain and have read-and-write privileges to objects in the subdomain, you can perform read-and-write operations successfully even if the subdomain is not assigned to you. You only need to switch to the subdomain and perform read-and-write operations on the objects within the subdomain. However, if you are a parent domain user with read-only permissions to objects, then you can perform only read operations on the objects in the subdomain.



NOTE: In read-only mode, you cannot modify or delete objects. For example, in read-only mode, you cannot modify a device that is in the parent domain if you are logged in to the subdomain, even if you have the permissions to do so.



NOTE: Objects across domains cannot share the same name. That is, you cannot create objects with the same name on more than one domain.

You can move objects from one domain to another. For example, use the **Assign to Domain** task in the Device Management workspace to move a device to another domain. On the User Accounts page, you can use the modify workflow to move a user to another domain.

To access workspaces on an application that is running on Junos Space Network Management Platform, these workspaces should be domain aware. Otherwise, this application appears disabled in the subdomain. Only domain-aware workspaces of an application can be accessed from the subdomains. When you switch domains, it is likely that you lose access to workspaces in an application if the application is not domain aware.

In Junos Space Release 13.1 and earlier, using permission labels, administrators partition a device into subgroups and assign these subobjects to different users. From Junos Space Release 13.3R1 onward, device partitions are used to replicate this behavior. Device partitions are supported only on M Series and MX Series routers.

You can partition a device from the Device Management workspace. When you assign a domain, you can select a device or its partition. You can assign each partition of a device to a different subdomain. That is, you cannot assign more than one partition of a device to the same subdomain. For example, consider device D1 with partitions P1, P2, and P3, device D2 with partitions P1a and P2a, and Global, dom1, and dom2 to be the available domains in Junos Space. The following assignment of partitions is valid:

P1 to dom1, P1a to dom1, P2 to dom2, P2a to dom2, P3 to Global (default).

The following assignments are invalid:

P1 and P2 to dom1 or P1a and P2a to dom2

To assign a partition to a subdomain, the root device needs to be in a parent domain.

When you right-click a device partition, actions that you can or cannot perform are listed in [Table 75 on page 560](#):

Table 75: Actions Supported on Device Partitions

Action Group	Action Name	Device Partition Support	Notes
Device Configuration	Review/Deploy Configuration	No	
	View/Edit Configuration	No	
	View Active Configuration	Yes	Configuration details are not filtered on the basis of the partitioning.
	Resolve Out-of-band Changes	No	
	View/Assign Shared Objects	No	
	View Configuration Change Log	Yes	Configuration details are not filtered on the basis of the partitioning.
	View Template Deployment	No	
	View/Edit Unmanaged Device Configuration	No	
Device Inventory	Export Physical Inventory	No	
	View Associated Scripts	Yes	
	View License Inventory	No	
	View Logical Interfaces	Yes	
	View Physical Interfaces	Yes	
	View Physical Inventories	Yes	
	View Script Execution	Yes	
	View Inventory Change	Yes	
	View Software Inventory	No	
Device Operations	Create LSYS	No	LSYS should be managed only on the root device.
	Delete Devices	No	You cannot delete a device partition from the subdomain.
	Looking Glass	No	
	Put in RMA State	No	This action can be performed only on the root device.

Table 75: Actions Supported on Device Partitions (*continued*)

Action Group	Action Name	Device Partition Support	Notes
	Reactivate from RMA	No	This action can be performed only on the root device.
	Synchronize with Network	No	This action can be performed only on the root device.
	Execute Script	Yes	
	Apply CLI Configlet	Yes	
Device Access	Modify Authentication	No	This action can be performed only on the root device.
	Launch Device WebUI	No	This action can be performed only on the root device.
	SSH to Device	No	This action can be performed only on the root device.
	Resolve Key Conflict	No	This action can be performed only on the root device.
Managed Customized Attribute		No	
Delete Private Tags		No	
Tag It		No	
Un Tag It		No	
View Tags		No	
Filter by CSV		Yes	
Clear All Selection		Yes	

Use the **Assign to Domain** task from the Actions menu to reassign a selected device or device partition from one domain to another.

To summarize:

- Objects can belong to only one domain.
- Objects across domains cannot share the same name.

- Users in a domain can view objects above them in read-only mode only if the higher domain allows its objects to be viewable in its subdomains.
- Users can view objects in a subdomain as well as write to those objects if provided with the appropriate permissions.
- Objects that are created by an action that you perform in a domain are assigned to the same domain.
- Objects can be moved from one domain to another.
- Users cannot modify or delete objects that are in read-only mode even if they have permissions to modify those objects by virtue of the role assigned to them.

Consider the following points when you use the following workspaces and inventory landing pages:

- **Templates**—Templates and template definitions are automatically created in the domain that you are currently in. During template creation, you can select the template definition from the same domain or parent domain if you have access to the parent domain. You can deploy templates on devices that are in the same domain or to a domain that is below the current operating domain.

From the inventory page, you can view the objects that are inherited from the parent domain.

Use the **Assign to Domain** task from the Actions menu to reassign a selected template or template definition from one domain to another.

- **Configlets**—Configlets are assigned to the domain that you are currently in. You can apply configlets to devices belonging to the same domain or to a domain that is below the operating domain. You can assign and deploy configlets that are inherited from the parent domain to the devices in the current domain.

From the inventory page, you can view the objects that are inherited from the parent domain.

Use the **Assign to Domain** task from the Actions menu to reassign a selected configlet from one domain to another.

- **Images**—Images are assigned to the domain that you are currently in. You can stage, deploy, or perform any action on images to only those devices belonging to the same domain or to a domain that is below the operating domain. You can use images that are inherited from the parent domain and perform an action on them on devices in the current domain, such as staging the inherited images to a device in the current domain.

From the inventory page, you can view the objects that are inherited from the parent domain.

Use the **Assign to Domain** task from the Actions menu to reassign a selected image from one domain to another.

- **Scripts**—Scripts are assigned to the domain that you are currently in. You can stage, deploy or perform any action on scripts to only those devices belonging to the same domain or to a domain that is below the operating domain. You can use scripts that

are inherited from the parent domain and perform an action on them on devices in the current domain, such as staging the inherited scripts to a device in the current domain.

From the inventory page, you can view the objects that are inherited from the parent domain.

Use the **Assign to Domain** task from the Actions menu to reassign a selected script from one domain to another.

- **Configuration files**—Configuration files are created in the same domain to which the devices belong. If the devices are moved from one domain to another, then the configuration files are also automatically moved to the respective domain. The Configuration Files workspace does not display objects inherited from the parent domain.
- **Jobs**—Jobs are associated with the domain from which the user has initiated the jobs.
- **Audit logs**—Audit logs are generated in the domain from which the user has initiated the actions.
- **Global search**—Global search displays objects that match the search query from the current domain, child domains, and parent domain, if the user has read-only access to the parent domain. If an object in the search results is in a different domain than the one the user is currently in, the hyperlink to the object in the search results is disabled.
- **Roles**—The Role Based Access Control workspace and hence the Roles Inventory Landing Page is not available in the subdomains.
- **Users**—You can create users only when you are logged in to the global domain. At the time of creating a user, you can assign the user to a subdomain.
- **Administration**—The complete Administration workspace is available only if you are logged in to the global domain. Administration > Tags is available for all users in all domains.
- **Reports**—Report definitions are assigned to the domain in which they are created. You can generate reports by using the definition in the inherited domain or in the current domain. That is, you can generate reports in the domain that you are currently in and also in domains that you have access to, including the inherited domains.

From the inventory page, you can view the report definitions that are inherited from the parent domain.

Migration and Backward Compatibility

The permission labels that you use in Junos Space 13.1 and earlier are replaced with domains from Junos Space Release 13.3R1 onward. When you migrate to Junos Space Release 13.3R1 or later, consider the following points if you assigned permission labels to objects in previous versions of Junos Space. This is a general guideline and might require administrator intervention after the migration because it might not be possible to capture the exact intent of the permission label assignment.



NOTE: Objects with no permission labels are assigned to the global domain by default.

- When you have assigned one permission label per object in versions prior to Junos Space Release 13.3R1—After the upgrade, a domain is created for each label and all the objects that were previously assigned to this label are reassigned to the newly added domain. For example, consider *UserA* and *DeviceA* that were assigned to permission label *DomA* in Junos Space 13.1. When you migrate to Junos Space 13.3R1 or later, a new domain *DomA* is created automatically, and *UserA* and *DeviceA* are assigned to the *DomA* domain by default.
- When more than one permission label is assigned to an object—After the upgrade, Junos Space adds a new domain by appending the permission label names and assigns the object to this newly added domain. For example, if *DeviceB* is assigned to permission labels *DomA* and *DomB* in Junos Space 13.1, then after the upgrade a new domain *DomA + DomB* is created and *DeviceB* is assigned to this newly added domain.
- When you use permission labels to achieve subobject permissions—If a device has subobject permissions, then after the upgrade, the device partition is created out of the sub objects. These partitions are then assigned to the global domain and not assigned to any subdomain.

Related Documentation • [Working with Domains on page 564](#)

Working with Domains

You can add, modify, or delete a domain from the Role Based Access Control > Domains inventory landing page. This workspace is accessible only when you are logged in to the global domain, which means that you can add, modify, or delete a domain only from the global domain. You need the Domain Administrator role to perform these actions. If you are assigned a role that does not allow you to perform these actions, then you cannot perform them. If you are a User Administrator creating a custom role, you can assign the privileges of a Domain Administrator to the new user.



NOTE: The Role Based Access Control workspace is visible only if are logged in to the global domain. It is not visible in the subdomains.

-
- [Adding a Domain on page 564](#)
 - [Modifying a Domain on page 566](#)
 - [Deleting Domains on page 567](#)

Adding a Domain

You can add a domain from the Domains workspace. By default, this domain is added under the global domain. When you add a domain, you can choose to allow users in this domain to have read-only access to the parent domain. If you choose to do so, all users in the subdomain can view objects of the parent domain in read-only mode.



NOTE: Only two levels of hierarchy are supported: global domain and other domains that you might add under the global domain.

To add a domain:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Domains**.

The Domains page appears. This page consists of two panes. The left pane lists the domains that are currently available in Junos Space Network Management Platform. The right pane displays details about the domain that you have selected on the left pane. Because the **Global** domain is selected by default on the left pane, the right pane displays details about the global domain.

2. On the left pane, click the **Add** icon to add a new domain.

The Add Domain page appears, displaying the fields of the Domain Information area.

3. In the **Domain Name** field, enter the name of the domain.

The domain name cannot exceed 255 characters and cannot contain comma, double quotes, or parenthesis. Also, the name cannot start with a space.

4. (Optional) Select the **Allow users of this domain to have read-only access to parent domain** check box if you want to allow users of this domain to have read-only access to the objects in the parent domain.

5. (Optional) In the **Description** field, add a description that will help you recollect the purpose of the domain at a later point of time.

6. Click **Next**.

The Assign Users page appears, displaying all Junos Space users except the super user.

7. Select one or more users to assign to this domain.

If you want to assign all users to this domain, then select the **Select all items across all pages** check box.

8. Click **Next**.

The Assign Devices page appears, displaying all devices that are discovered in Junos Space.

9. Select one or more devices to assign to this domain.

If you want to assign all devices to this domain, then select the **Select all items across all pages** check box.

To quickly locate the devices, perform one of the following tasks:

- Search for devices by using the **Search** field. Type the first few letters of the device name in this field and press Enter to display devices that match the search criteria.
- Filter data on any of the columns displayed by selecting the columns on the **Column Filter** field and entering the filtering criteria for the selected columns.
- Use the **Tag Filter** list and select the tags to view only those devices that are tagged using specific tags.
- Use a CSV file containing a list of devices by clicking the **CSV Filter** option.

10. Click **Finish**.

The new domain is added in Junos Space and you are returned to the Domains page.

When you add a domain, audit log entries are automatically generated.

Modifying a Domain

Only a user with the Domain Administrator role can modify a domain.

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Domains**.

The Domains page appears.

2. Select the domain that you want to modify from the left pane.

The right pane displays details about the selected domain.

3. Click the **Modify** icon on the left pane.

The Modify Domain dialog box appears.

4. Make the necessary changes to the domain by using the Modify Domain dialog box.

You can modify the domain name and description, and allow or prevent users to have or from having read-only access to objects in the parent domain.

5. Click **Save** to close the Modify Domain dialog box.

6. On the right pane, assign or unassign users as required.

To assign users to this domain:

- a. Click the (+) icon (**Assign Users**) on the right pane.

The Assign Users page appears, displaying the Junos Space users except the super user and users who are not previously associated with this domain.

- b. Select one or more users to assign to this domain

You may want to sort the data in any of the columns on the Assign Users page to quickly identify the users.

- c. Click **Assign**.

You are returned to the Domains page, which displays the users that you added to this domain.

To unassign users from this domain:

- a. Select users whom you no longer want to associate with this domain.
- b. Click the (–) icon (**Unassign Users**) on the right pane.

The selected users are unassigned from this domain. However, the following error message is thrown even if one of the selected users belong only to this domain and not to any other domain. The delete action fails.

User needs to be assigned to atleast one domain

7. Click the **Assigned Devices** tab to assign devices to this domain. Use the (+) icon to achieve this task.

When you modify a domain, an audit log entry is automatically generated.

Deleting Domains

Only a user with the Domain Administrator role can delete a domain.

When you delete a domain, take the following points into consideration:

- All users who are logged in to the domain are logged out.
- The domain is locked and users cannot move or log in to that domain unless the job fails.
- No objects must belong to the domain that is being deleted. You need to purge and archive audit logs and job data as well as move or delete devices and all other objects in that domain to another domain before you proceed with the deletion. You must trigger the deletion of a domain only after you ensure that there are no objects in that domain. If objects exist in the domain, the deletion job fails and a list of objects to be deleted is provided in the job description.
- Another administrator cannot create a domain with the same name as the domain that is deleted when the domain deletion job is in progress.
- You cannot delete the global domain.

To delete a domain:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Domains**.

The Domains page appears.

2. Select the domain that you want to delete from the left pane.
3. Click the **Delete** icon on the left pane.

A confirmation dialog box appears.

4. Click **Yes** on the confirmation dialog box to delete the domain.

An information dialog box appears, displaying the job ID of the deletion job. Click the job ID to see whether the deletion of the domain is successful. If the job failed, then double-click the deletion job to determine the reasons for failure.

When the deletion of a domain fails, use the reasons listed in the job description of the domain deletion job to resolve the issue. For example:

1. On the Junos Space Network Management Platform user interface, select **Jobs > Job Management**.

The Job Management page appears.

2. Double-click the domain deletion job whose details you want to view.

The Delete Domain Detail Report page appears. On this page, you see something similar to the following text in the Description column:

1. **Delete or reassign following users before deleting domain: {test-user-1, test-user-2, }**
 2. **3 Device Object object[s] present in domain. Please remove or assign to another domain before deleting.**
 3. **162 Physical Interface Object object[s] present in domain. lease remove or assign to another domain before deleting.**
 4. **80 Physical Inventory Object object[s] present in domain. lease remove or assign to another domain before deleting.**
 5. **24 Logical Interface Object object[s] present in domain. lease remove or assign to another domain before deleting.**
3. Analyze the report and resolve the issue. In this example, resolve point 2 in the previous step, which is likely to address points 3, 4, and 5 because points 3, 4, and 5 are related to the devices in point 2.

You may encounter this error if a device is attached to only a single domain and you are trying to delete that domain. To resolve this error, identify the devices that are assigned to this domain from the Domains workspace and reassign the devices to another domain. In this example, assume that one of the devices assigned to the domain that you are trying to delete is DeviceA.

To reassign DeviceA to the global domain:

- a. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

- b. Select DeviceA.
- c. Click **Assign to Domain** from the Actions menu.

The Assign to Domain page appears, displaying all domains on the Junos Space server.

d. Click **Global**.

e. Click **Assign**.

The selected device is reassigned to the global domain.

4. Resolve point 1, which states that:

Delete or reassign following users before deleting domain: {test-user-1, test-user-2, }

You may encounter this error if a user is attached to only a single domain and you are trying to delete that domain. To resolve this error, identify the users assigned to this domain from the Domains workspace and reassign the users to another domain. In this example, reassign test-user-1 to the global domain.

a. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts page appears.

b. Select test-user-1.

c. Click the **Modify User** icon.

The Modify User page appears.

d. Click **Domain Assignment** on the right pane of the Modify User page.

e. Select the **Global** check box.

f. Click **Finish**.

The selected user is reassigned to the global domain.

Repeat this procedure for test-user-2. Then repeat Step 3 for the remaining devices.

5. Try deleting the domain now. You should be able to delete the domain because you have resolved the issues that were preventing you from deleting the domain.

When you delete a domain, an audit log entry is automatically generated.

Related Documentation

- [Managing Domains Overview on page 557](#)

CHAPTER 59

Manage Users

- [Creating User Accounts on page 571](#)
- [Disabling and Enabling Users on page 581](#)
- [Viewing Users on page 582](#)
- [Modifying a User on page 587](#)
- [Deleting Users on page 590](#)
- [Unlocking Users on page 592](#)
- [Changing Your Password on Junos Space on page 593](#)
- [Clearing User Local Passwords on page 594](#)
- [Viewing User Statistics on page 595](#)

Creating User Accounts

The Super Administrator and the User Administrator can create Junos Space Network Management Platform user accounts that specify the credentials, predefined roles, and domain allowing users to log in and use Junos Space applications, workspaces, and tasks within a specified domain.

For credential-based user authentication, each user account must include:

- Login ID
- Password
- First name
- Last name
- Roles, which determine the tasks that a user can perform within applications and workspaces
- Domains within which the user can operate

For certificate-based user authentication, each user account must include:

- Login ID
- First name
- Last name

- X509 Cert File
- Roles, which determine the tasks that a user can perform within applications and workspaces
- Domains within which the user can operate

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.

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 account creation is subdivided into three areas—**General**, **Role Assignment**, and **Domain 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.

Creating a New User Account

The Super Administrator or the User Administrator creates the user accounts in Junos Space Network Management Platform and assigns roles to these accounts. These roles determine the tasks that users can perform in Junos Space Network Management Platform.

As an administrator, you have the option to assign a temporary or regular password to a new user or to an existing user whose password has expired. Consider the points mentioned in [Table 76 on page 572](#) before assigning a temporary or regular password to a user:

Table 76: Differences Between Temporary and Regular Passwords

Temporary Password	Regular Password
Users must change their temporary passwords at first login.	Users need not change their passwords at first login.
When temporary passwords expire, users cannot access the Junos Space server. To access the Junos Space server, users need to use the new passwords that the administrator has generated and shared with them. Users cannot change their passwords on their own.	When regular passwords expire, users can change their passwords on their own after logging in to the Junos Space server.
Password expiry time is configured at the user level. By default, temporary passwords expire after 24 hours.	Password expiry time is configured at the global level from the Administration workspace. This expiry time applies to all users with regular passwords. For more information about configuring parameters related to regular passwords, see “Configuring Password Rules for Junos Space Network Management Platform” on page 714 .

To create a new user account:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts page appears.

2. Click the **Create User** icon on the toolbar above the application data to display the Create user page.

The Create user page appears, displaying the fields for the General area.

3. In the **Login ID** field, 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 matches 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. (Optional) Select the **Generate a temporary password** check box if you want to generate a temporary password for the user. Generation of temporary passwords is supported only in local-mode authentication. It is not supported in “Remote-Local Authentication” or “Remote Authentication” modes.

As an administrator, you may want to generate a random password for a new user or when the password expires for an existing user. Users must change their temporary passwords when they log in for the first time. Users with temporary passwords are not allowed to use any of the features in Junos Space Network Management Platform unless they replace their temporary passwords with new passwords.

When you generate a temporary password for a user, consider configuring the following fields related to the temporary password:

- **Temporary password will expire after**—Specify the duration after which the temporary password expires. The user must log in to Junos Space within this duration and change the temporary password. Otherwise, after the expiry of the password, the user is not allowed to log in. When the temporary password expires, Junos Space displays the following message:
Your password has expired.
Please contact your administrator.

The user must request the administrator for a new password.

By default, the temporary passwords expire after 24 hours of its generation. The administrator can enter a value from 1 through 10,000.

- **Temporary Password**—Displays the temporary password generated by the Junos Space server. To generate another password, click **Generate** next to this field. The new generated password is displayed in this field.

- **Email password to user**—Select this check box to e-mail the generated temporary password to the user. This check box is disabled if the SMTP server is not configured.

If the e-mail does not reach the user or the password is lost, the administrator needs to generate a new temporary password. There is no option to resend the old temporary password.



TIP:

For the Junos Space server to automatically send the temporary password and expiry date by e-mail to the user, ensure that you configure:

- The e-mail ID of the user in the **Email** field on the Create user page (the page that you are currently in).
- The SMTP server that receives the e-mail from the Junos Space server and routes it to the intended recipient.

You configure the SMTP server on the **Administration > SMTP Servers** inventory landing page. After configuring the SMTP server, test the connection between the Junos Space server and the SMTP server to ensure that communication between the servers is established. For more information about SMTP server configuration and how to test the configuration, see [“Adding an SMTP Server” on page 776](#) and [“Managing SMTP Servers” on page 775](#).

5. (Optional) Display the rules for password creation by mousing over the information icon (small blue *i*) next to the Password field. For information about configuring the password rules, see [“Configuring Password Rules for Junos Space Network Management Platform” on page 714](#).

6. In the **Password** field, enter the local password.

This field is disabled (grayed out) if you have chosen to generate the temporary password.



NOTE: All passwords in Junos Space Network Management Platform are case-sensitive.

7. In the **Confirm Password** field, reenter the password to confirm the password.

This field is disabled (grayed out) if you have chosen to generate the temporary password.

8. In the **First Name** field, enter the user's first name.

The name cannot exceed 32 characters.

9. In the **Last Name** field, enter the user's last name.

The name cannot exceed 32 characters.

10. (Optional) In the **Email** field, enter the user's e-mail address. However, you have to enter an e-mail address in this field if you have opted to e-mail the temporary password to a user by selecting the **Email password to user** check box.

This need not be the same as the login ID, if the login ID is an e-mail address.

Ensure that the e-mail ID that you enter is valid and uses the following format:
user@domain.

11. (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** field just below this check box. For more information about how to configure this limit globally, see [“Limiting User Sessions” on page 579](#).

12. (Optional) In the **Maximum concurrent UI sessions** field, 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. The default value for this field is 5. This means that a user can have five concurrent sessions running at the same time. For more information about how to configure this limit globally, see [“Limiting User Sessions” on page 579](#).

Typically, this text box is unavailable (that is, when the Use global settings check box remains selected). To make any configuration changes in the Maximum concurrent UI sessions field, 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 on the number of concurrent UI sessions allowed per user. However, the system performance may be degraded if you allow too many sessions.

13. (Optional) In the **Image File** field, upload the user's photo ID from your local file system:

- 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.

14. (Optional) In the **X509 Cert File** field, upload the user's X.509 certificate file. If you upload a certificate, then the user is authenticated on the basis of the user's certificate instead of the user's login credentials (username and password). For more information about certificate-based user authentication, see [“Certificate Management Overview” on page 745](#).

- 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.

If you do not want to assign the user roles 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**.

15. To assign roles to the new user, click **Role Assignment** on the upper right, and perform one of the following tasks:

- 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 on the **Selected roles** list. You can modify the new user's role assignments by adding roles to or removing roles from the **Selected Roles** column.

- 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 when you 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. That is, you can view the tasks that the role allows the user to perform on 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 553](#).



TIP: When you install various applications in Junos Space, predefined roles for each of these applications are made available to you, and you can view these roles from the Role Based Access Control workspace. So, when you want to restrict a user to a specific application, make sure that you assign the role specific to that application while creating or modifying the user.



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.

16. To assign domains to the new user, click **Domain Assignment** on the upper right. All available domains are displayed.

17. Select the domains to which the new user should be assigned.

The user should be assigned to at least one domain. If you do not assign any specific domain to the user, then by default, the user is assigned to the global domain.

18. 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 User Accounts inventory page. The following information is displayed for the newly created user account on this page:

- **User Name**—Username of the user, which is used for logging in
- **First Name**—First name of the user
- **Last Name**—Last name of the user
- **Email**—E-mail ID of the user
- **User Type**—Whether the user is configured locally or remotely. For the user that you just added, this column displays **Local** to distinguish this user as a local user.
- **Status**—Whether the user is enabled or disabled. By default, newly added users are always enabled.

A disabled user cannot log in to the Junos Space server.

- **Password Status**—Whether the password is active or expired. One of the following values is displayed for each user:
 - **Active**—User is given a regular password and the password is active.
 - **Expired**—User's regular password has expired. Such users can log in to Junos Space and change the passwords on their own.
 - **Temporary Expired**—User's temporary password has expired. Such users can log in to Junos Space only if the administrator gives them a new password.
 - **Temporary**—User's temporary password is active. The user must log in to Junos Space and change the temporary password before it expires.
- **GUI/API Access**—Whether the user has GUI and API access
- **Locked Out**—Whether the user is locked out

Yes on this column indicates that the user is locked out for at least one IP address. If a user tries to log in to the system from an IP address that is locked, the following message is displayed:

This account is Locked. You can't Log in.

The user must then request the administrator to unlock the account.

No on this column indicates that the user is not locked out.

All columns support sorting of data in ascending and descending order. Filtering of data is supported in all columns except the Password Status column.



NOTE: If the **Email password to user** check box is enabled during user creation, the "Mail user password" job is triggered and an audit log entry is generated.

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 the 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.

The audit log entry also includes the reason for login failure:

Login Failed. Maximum concurrent user session limit is reached.



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 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 the 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 users):

1. On the Junos Space Network Management Platform user interface, select **Administration > Applications**.

The Applications page appears.

2. Select **Network Management Platform**.
3. Select **Modify Application Setting** from the **Actions** menu.

The Modify Network Management Platform Settings page appears.

4. Click **User**.
5. In the **Maximum concurrent UI sessions per user** field, 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 on 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. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts page appears.

2. Click the **Create User** icon on the toolbar above the application data.

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** field.

4. (Optional) In the **Maximum concurrent UI sessions** field, 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 on 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 Junos Space Network Management Platform users, from the User Accounts page, select the user and click the **Modify User** icon to make any changes to the concurrent UI sessions limit for that user.



NOTE: The changes that you make 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 login only.

For troubleshooting, see the `/var/log/jboss/servers/server1/server.log` file, which captures any internal errors. Also, see the audit logs, which captures the following information:

- Configuration changes made by the Administrator to the global concurrent UI sessions limit
- When the global configuration is overridden at the user level
- When the global configuration is overridden at the user level
- When the concurrent UI sessions limit is reached for a user

Related Documentation

- [Configuring Users to Manage Objects in Junos Space Overview on page 521](#)
- [Predefined Roles Overview on page 521](#)
- [Changing Your Password on Junos Space on page 5](#)
- [Modifying a User on page 587](#)
- [Deleting Users on page 590](#)
- [Viewing Users on page 582](#)

Disabling and Enabling Users

Disable a user to prevent the user from logging in to the system. By default, all users are enabled.



NOTE:

- You cannot disable your own user account.
- You cannot disable Super user. However, you can disable a user with the Super Administrator role.

From the status of the user, which is displayed in the **Status** column on the User Accounts inventory landing page or in the **Status** field on the User Detail Summary page, you can determine whether the user account is enabled or disabled.

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 off the user and displays to the user a message saying that the user account is disabled. In both cases, when a disabled user attempts to log in, an audit log entry is automatically generated. A sample audit log entry that is generated when a user whose account is disabled tries to log in is as follows:

Login Failed. The user is disabled.

To disable or enable one or more users:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > 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 on 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** or **Enable**, respectively.

All selected user accounts are disabled or enabled.

When you enable or disable a user, an audit log entry is automatically generated. To view details about users whom you have enabled or disabled from the audit log, double-click the audit log entry. For example, double-click the **Disable Users** audit log entry in the **Task** column. The Audit Log Detail page appears, which displays the users that are disabled. Select a user from the **Affected Objects** section. Details about the user are displayed in the **Affected Object Detail** section to the right of the page.

Related Documentation

- [Creating User Accounts on page 571](#)
- [Modifying a User on page 587](#)
- [Viewing Users on page 582](#)
- [Junos Space Audit Logs Overview on page 603](#)

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 571](#). Users have Junos Space access based on predefined user roles (see [“Predefined Roles Overview” on page 521](#)). For more information about how to manipulate inventory page data, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

This topic describes how to view the inventory of users and their details. To do this, select **Role Based Access Control > User Accounts**.

The User Accounts page appears.

Users are displayed in a table sorted, by default, by username. 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, Status, Password Status, and Locked Out.

The status bar at the bottom of the page shows the range of objects that are displayed. For example, you might see *Displaying 1-30 of 113*. In addition, the **Show items** list enables you to select the number of items to display per page: 10, 20, 40, 60, 80, 100, 200.

The filter function, described in this topic, enables you to get around the difficulty of not being able to view all users on a single page.

- [Sorting Columns on page 583](#)
- [Displaying or Hiding Columns on page 583](#)
- [Filtering on Columns on page 584](#)
- [Viewing User Details on page 585](#)
- [Performing Actions on Users on page 586](#)

Sorting Columns

The columns in the User Accounts table (that is on the User Accounts inventory landing page) can be sorted by ascending or descending order.

To sort the contents of a column:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts page appears, displaying the users in tabular form.

2. Click the down arrow to the right of any column heading.

A list with the following menu options appears:

- **Sort Ascending**
 - **Sort Descending**
 - **Columns**
 - **Filters**
3. 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 User Accounts table (that is on the User Accounts inventory landing page) can be displayed or hidden as required.

To display or hide a column:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts page appears, displaying the users in tabular form.

2. Click the down arrow to the right of any column heading.
3. Select **Columns**.

A list with menu options corresponding to all the available column headings appears with a check box next to each heading. The check boxes for the headings that are displayed are selected; those that are hidden are not selected.

4. Select or deselect the headings as desired.

The tabular view changes to reflect your choices.

Filtering on Columns

The contents of the columns in the User Accounts table (that is on the User Accounts inventory landing page) can be filtered as required.

To filter on a column:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts page appears, displaying the users in tabular form.

2. Click the down arrow to the right of any column heading.
3. Select **Filters**.

The filter field appears, with a **Go** button to the right of it.

4. Enter or select the filter criteria and click **Go**.

On applying the filters, 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.

5. To remove a filter, click the [X] icon to the right of the filter criteria shown just above the table. For more information about filtering on columns, see “Filter Submenus” in *Inventory Landing Page*.

Viewing User Details

To view more detailed user information:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.
2. Perform one of the following tasks:

- Select a user and click the **Display Quick View** icon on the menu bar.

The following information is displayed to the right of the selected user:

- Login ID
- First Name
- Last Name
- Email
- User Type
- Locked Out
- Password Status

For more information about these fields, see [Table 77 on page 585](#).

To hide the quick view, click the **Hide Quick View** icon on the menu bar.

- Double-click a user row in the table.

The User Detail Summary page appears, showing the information described in [Table 77 on page 585](#).

Table 77: User Detail Summary Page

Field Name	Description
Login ID	Login username. This could be an e-mail address, but it need not match the e-mail address that might be provided in the Email field for that username.
First Name	First name of the user
Last Name	Last name of the user
Email	(Optional) User's e-mail account. The e-mail address provided here need not match the login ID, if the login ID is also an e-mail address.
User Type	Whether the user is created manually (Local) or automatically by Junos Space Network Management Platform through remote login (Remote). For more information about local and remote users, see the flowcharts in " Configuring a RADIUS Server for Authentication and Authorization " on page 764.
Status	Whether the user is Enabled or Disabled . Users are enabled by default. Disabling a user is not the same as deleting a user. A user whose account is disabled cannot log in to the Junos Space server.

Table 77: User Detail Summary Page (*continued*)

Field Name	Description
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 to determine the maximum number of concurrent UI sessions permitted for the user
Maximum concurrent UI sessions	Maximum number of concurrent UI sessions permitted for the user. If this field is set, then this value overrides the global settings.
Locked Out Status	Whether a user is locked out. A locked-out user cannot log in to the Junos Space server. Such users must request the administrator to unlock their user accounts.
Password Status	Whether a user's password is expired or active. The term "Temporary" is displayed for temporary passwords.
Assigned Roles	Predefined user roles assigned to the user
Assigned Domains	Domains to which the user is assigned. Users can access only those objects within the domain to which they are assigned. By default, all users are assigned to the global domain, if the users are not assigned to a specific domain.
Role Summary	Name of the applications to which the roles belongs, and list of permissions attached to the roles

To close the User Detail Summary page, click **OK** at the bottom of this page or the [X] icon in the upper-right corner of this page.

Performing Actions on Users

You can perform the following actions from the Users Accounts page:

- **Modify User**—See [“Modifying a User” on page 587](#).
- **Delete Users**—See [“Deleting Users” on page 590](#).
- **Clear Local Passwords**—See [“Clearing User Local Passwords” on page 594](#).
- **Disable Users and Enable Users**—See [“Disabling and Enabling Users” on page 581](#).
- **Unlock Users**—See [“Unlocking Users” on page 592](#).
- **Delete Private Tags**—Delete tags that you created.
- **Tag It**—See [“Tagging an Object” on page 793](#).
- **UnTag It**—See [“Untagging Objects” on page 794](#).
- **View Tags**—See [“Viewing Tags for a Managed Object” on page 794](#).
- **Clear All Selections**—All selected users on the User Accounts inventory page are deselected.

- Related Documentation**
- [Configuring Users to Manage Objects in Junos Space Overview on page 521](#)
 - [Creating User Accounts on page 571](#)
 - [Deleting Users on page 590](#)
 - [Modifying a User on page 587](#)
 - [Viewing User Statistics on page 595](#)
 - [Tagging an Object on page 793](#)
 - [Viewing Tags for a Managed Object on page 794](#)

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 Domain 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. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > 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 582](#).

You can modify only one user account at a time.

3. From the menu bar above the table, click the **Modify User** icon (the pencil icon).

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 generate a temporary password, select the **Generate a temporary password** check box. You generate passwords for new users or existing users whose passwords have expired. Generation of temporary passwords is supported only in local-mode authentication. It is not supported in “Remote-Local Authentication” or “Remote Authentication” modes.

To generate a temporary password, configure the following fields:

- **Temporary password will expire after**—Specify the duration after which the temporary password expires. The user must log in to Junos Space within this duration and change the temporary password. Otherwise, after the expiry of the password, the user is not allowed to log in. When the temporary password expires, Junos Space displays the following message:

Your password has expired.

Please contact your administrator.

The user must request the administrator for a new password.

By default, the temporary passwords expire after 24 hours of its generation. The administrator can enter a value from 1 through 10,000.

- **Temporary Password**—Displays the temporary password generated by the Junos Space server. To generate another password, click **Generate** next to this field. The new generated password is displayed in this field.
- **Email password to user**—Select this check box to e-mail the generated temporary password to the user. This check box is disabled if the SMTP server is not configured.

If the e-mail does not reach the user or the password is lost, the administrator needs to generate a new temporary password. There is no option to resend the old temporary password.



TIP:

For the Junos Space server to automatically send the temporary password and expiry date by e-mail to the user, ensure that you configure:

- The e-mail ID of the user in the **Email** field on the Create user page (the page that you are currently in).
- The SMTP server that receives the e-mail from the Junos Space server and routes it to the intended recipient.

You configure the SMTP server on the **Administration > SMTP Servers** inventory landing page. After configuring the SMTP server, test the connection between the Junos Space server and the SMTP server to ensure that communication between the servers is established. For more information about SMTP server configuration and how to test the configuration, see [“Adding an SMTP Server” on page 776](#) and [“Managing SMTP Servers” on page 775](#).

- 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 Rules for Junos Space Network Management Platform” on page 714](#).
- To change the username, enter a new name in the **First Name** and **Last Name** fields.
- To change the e-mail account, enter a new e-mail address in the **Email** field.
- To change the maximum number of concurrent UI sessions that should be allowed for this user:
 - a. Clear the **Use global settings** check box.
 - b. Enter the number of sessions in the **Maximum concurrent UI sessions** field.

You can enter a value from 0 through 999. Entering 0 (zero) means that there is no restriction on the number of concurrent UI sessions allowed for this user. However, the system performance may be degraded if you allow unlimited sessions.

- (Optional) To upload an image file from your local file system:

- a. Use the **Browse** button adjacent to the **Image File** field 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.

- (Optional) To upload the user's X.509 certificate file from your local file system:

- a. Use the **Browse** button adjacent to the **X509 Cert File** field 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. If you upload a certificate, then the user is authenticated based on the user's certificate instead of the user's login credentials (username and password). For more information about certificate-based user authentication, see ["Certificate Management Overview" on page 745](#).

5. To add or remove role assignments:



TIP: When you install various applications in Junos Space, predefined roles for each of these applications are made available to you, and you can view these roles from the Role Based Access Control workspace. So, when you want to restrict a user to a specific application, make sure that you assign the role specific to that application while creating or modifying the user.

- a. Click **Role Assignment** on the upper right of the Modify User page, or click **Next** on the bottom right of the Modify User 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.
6. To add, remove, or change domain assignments:
 - a. Click **Domain Assignment** on the upper right of the Modify User page, or click **Next** on the lower right of the Modify User page.
 - b. Select the domains to which the new user must be assigned. By default, the user is assigned to the **global** domain.



NOTE: The user must be assigned to at least one domain.

7. 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.



NOTE: If the **Email password to user** check box is enabled during user modification, then "Mail user password" job is triggered and an audit entry is made to record this action.

Related Documentation

- [Configuring Users to Manage Objects in Junos Space Overview on page 521](#)
- [Creating User Accounts on page 571](#)
- [Deleting Users on page 590](#)
- [Viewing Users on page 582](#)

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. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts inventory page appears, displaying all user accounts in a table.

2. Select one or more users to delete.
3. From the menu bar above the table, click the **Delete Users** icon.

The Delete Users confirmation dialog box appears displaying only users with no pending jobs.

4. Retain the selection of the **Exclude users who have jobs in scheduled or inprogress state** check box, if you do not want to delete users who have initiated jobs that are in progress or who have scheduled jobs. That is, when you retain the selection of this check box, you delete only users with no pending jobs.



NOTE: You might notice that some of the users you selected for deletion do not appear on the Delete Users Confirmation dialog box. This is because these local and remote users are owners of scheduled, in progress, and recurring jobs and are by default excluded from deletion. To delete these users, you need to clear the **Exclude users who have jobs in scheduled or inprogress state** check box. When this check box is cleared, these users appear on the dialog box and are deleted when you click **Delete**. The **Jobs Scheduled/Inprogress** column on the Delete Users Confirmation dialog box displays **Yes** for users who have scheduled jobs or who have initiated jobs that are in progress.

Before you delete users with pending jobs, reassign these jobs to other active users within the same domain so as to ensure that these jobs are monitored and successfully completed. For example, reassign a recurring database backup job owned by UserA to UserB before deleting UserA. For more information about reassigning jobs, see [“Reassigning Jobs” on page 506](#).

5. Verify the list of users that you want to delete and click **Delete**. This button is disabled if there are no users to delete.

All selected user accounts that are displayed on the Delete Users Confirmation dialog box are removed from the Junos Space Network Management Platform database and the User Accounts inventory page.

Deleting users generate an audit log entry. The audit log entry records the users that were deleted.

To obtain details about the users who were deleted from an audit log entry:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs > Audit Log**.

The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using **Delete Users** keyword.

After filtering, the Audit Log page displays only the audit log entries that were generated when users were deleted.

3. Double-click an audit-log entry.

The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of users who were deleted and the **Affected Object Detail** section displays details about the deleted user.

4. Click **OK** on the Audit Log Detail page to exit this page.

You are returned to the Audit Log page.

- Related Documentation**
- [Creating User Accounts on page 571](#)
 - [Modifying a User on page 587](#)
 - [Viewing Users on page 582](#)

Unlocking Users

Junos Space Network Management Platform locks out users who enter more than the permitted number of incorrect passwords. If your user account is locked out, then you see the message **The account is Locked. You can't Log in.** when you try to log in to the Junos Space server. You can try logging in from another system or request the administrator to unlock your account.

By default, a user is locked out after four unsuccessful login attempts. As an administrator, you can decide after how many unsuccessful login attempts a user should be logged out. You can configure this setting from the Administration workspace. For more information about configuring this setting, see the **No. of unsuccessful attempts before lockout** parameter in [“Configuring Password Rules for Junos Space Network Management Platform” on page 714](#).

To unlock a user account:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts inventory page appears, displaying all user accounts in a table.

2. Select one or more locked users to unlock.



TIP: You can identify the locked-out users from the lock icon in the **Locked Out** column on the User Accounts inventory page.

3. Select **Unlock Users** from the Actions menu.

A confirmation dialog box appears displaying the users you have selected to unlock.

If **Unlock Users** is disabled, it means that one or more users that you have selected to unlock is not a locked-out user. Go to step 2 and select only locked-out users to proceed further.

4. Click **Unlock** on the confirmation dialog box to unlock the users.

The selected users are unlocked. These users can log in at the next login attempt.

Unlocking users generates an audit log entry with details about users that were unlocked.

To obtain details from an audit log entry about users who were unlocked:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs** > **Audit Log**.

The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using the **Unlock Users** keyword.

After filtering, the Audit Log page displays only the audit log entries that were generated when users were unlocked.

3. Double-click an audit log entry.

The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of users who were unlocked and the **Affected Object Detail** section displays details about the unlocked user.

4. Click **OK** on the Audit Log Detail page to exit this page.

You are returned to the Audit Log page.

Related Documentation

- [Role-Based Access Control Overview on page 519](#)

Changing Your Password on Junos Space

After you log in to Junos Space Network Management Platform, you can change your password through the User Preferences icon on the Junos Space banner. You do not require any particular Junos Space role to change your password.

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



NOTE: When you upgrade to Junos Space Network Management Platform 12.1 or later, the default standard takes effect immediately. All local users receive password expiration messages the first time they log in to Junos Space after the update.



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



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

To change your local password:

1. On the Junos Space Network Management Platform user interface, click the User Preferences icon on the right side of the Junos Space application banner.

The Change Local Password and Certificate dialog box appears.

2. In the **Old Password** text box, enter your old password.



NOTE: Display the rules for password creation by mousing over the information icon (small blue *i*) next to the **New Password** text box.

3. In the **New Password** text box, enter your new password.
4. In the **Confirm Password** text box, enter your new password again to confirm it.



NOTE: The fields on the X.509 Certificate tab are applicable when you want to use certificate-based authentication. If you are using password-based authentication, you can ignore these fields. For more information about certificate-based authentication, see [“Certificate Management Overview” on page 745](#) in the *Junos Space Network Management Platform User Guide*.

5. Click **OK**.

You are logged out of the system. To log in to Junos Space again, you need to use your new password. Other sessions logged in with the same username are unaffected until the next login.

Related Documentation

- [Logging In to Junos Space on page 3](#)

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 Administrator privileges.

To remove a user local password:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > 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.

This option is disabled (grayed out) if you try to clear the password for a local user.

The tooltip displays:

The following users are local only, so their passwords cannot be cleared: user1

The **Delete Users** dialog box appears.

4. Click **Clear Passwords**.

**Related
Documentation**

- [Viewing Users on page 582](#)
- [Creating User Accounts on page 571](#)
- [Modifying a User on page 587](#)
- [Creating a Remote Authentication Server on page 760](#)

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 595](#)

Viewing the Number of Users Assigned by Role

To view the percentage of total users that have been assigned to a predefined role:

1. On the Junos Space Network Management Platform user interface, click **Role Based Access Control**.

The Role Based Access Control 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 the segment of the chart that represents the role.

**Related
Documentation**

- [Role-Based Access Control Overview on page 519](#)
- [Viewing Users on page 582](#)
- [Creating User Accounts on page 571](#)
- [Deleting Users on page 590](#)

Manage Remote Profiles

- [Creating a Remote Profile on page 597](#)

Creating a Remote Profile

To create a remote profile:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Remote Profiles**.
The Remote Profiles page is displayed.
2. Click the **Create Remote Profile** icon on the menu bar.
The Create Remote Profile page appears, displaying the Role Assignment area.
3. In the **Name** field, enter a name for the remote profile.

The remote profile name cannot exceed 32 characters. The profile name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.).
4. In the **Description** field, enter a description for the remote profile.

The remote profile description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).
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 is able to access 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 **Next**.

The Domain Assignment area appears, displaying all available domains.

8. Select domains where the user can operate.
9. Click **Finish**.

A new remote profile is added.

Remote profiles can be modified, deleted, and tagged.



NOTE: A user is not 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 page. This information is logged in the audit log.

**Related
Documentation**

- [Predefined Roles Overview on page 521](#)
- [Managing Roles on page 551](#)
- [Modifying User-Defined Roles on page 554](#)
- [Deleting User-Defined Roles on page 555](#)
- [Creating User Accounts on page 571](#)

User Sessions

- [Terminating User Sessions on page 599](#)

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 are notified. The notification includes the date and time when the sessions will be terminated. As a user whose session will be terminated, you are automatically logged out at the scheduled date and time and redirected to the login page.



NOTE: You cannot terminate sessions of a user with the username *super*.

When you delete or disable a user in Junos Space Network Management Platform, the user's sessions is terminated 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.

To terminate user sessions:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Sessions**.

The User Sessions page appears. This page displays the username, the IP address from which the user has logged in, 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 page is displayed. This page 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 **Confirm** on the Terminate User Session page.

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 receive a pop-up message displaying the date and time you have specified for terminating their sessions.

When you terminate a user session, an audit log entry is automatically generated. On the Audit Log page (**Audit Logs > Audit Log**), you can filter data in the **Task** column by using the Terminate keyword to determine the number of terminated sessions, the name of the user that initiated this termination (from the **User Name** column), the IP address from which the user session is terminated (from the **User IP** column), the time at which the session is terminated (from the **Timestamp** column), and so on.

For a list of terminated users, click the **Job ID** link on the Audit Log page. The Job List page appears, displaying the terminated user sessions on the **Summary** column. However, if the job is a failure, double-click the job to determine the reason for failure.

From the Job List page, click **Back** to return to the Audit Log page.

**Related
Documentation**

- [Creating User Accounts on page 571](#)
- [Predefined Roles Overview on page 521](#)

PART 11

Audit Logs

- [View on page 603](#)
- [Archive / Purge on page 611](#)
- [Export on page 615](#)

CHAPTER 62

View

- [Junos Space Audit Logs Overview on page 603](#)
- [Viewing Audit Logs on page 604](#)
- [Viewing Audit Log Statistics on page 606](#)
- [Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel on page 608](#)

Junos Space Audit Logs Overview

The Audit Logs workspace of Junos Space Network Management Platform displays the login history of and tasks initiated by a user. Through this workspace, you can track login history, device-management tasks, services that were provisioned on devices, and so on. The Audit Logs workspace does not record non-user-initiated tasks, such as device driven activities (for example, resynchronization of network elements) and is not designed for debugging purposes. User-initiated changes that are made from the Junos Space CLI are logged but not recorded in audit logs.

Administrators can sort and filter 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 and logout activities 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 550](#)).



NOTE: Audit logging is not currently supported on Ethernet Design. However, from version 12.1 onward, audit logging is supported on Service Now.

Over time, the Audit Log Administrator archives 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 the volume of log data on Junos Space Network Management Platform, 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 611](#)
 - [Viewing Audit Logs on page 604](#)
 - [Exporting Audit Logs on page 615](#)

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 user-initiated tasks.

To view audit logs, you must have Audit Log Administrator privileges.



NOTE: Audit logging is not currently supported on Ethernet Design.

Junos Space Network Management Platform displays audit logs only in tabular view. For information about how to manipulate inventory page data, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

Viewing Audit Log Details

The Audit Log Detail 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, double-click a table row for the audit log entry. If the audit log entry includes a job ID link, click it to open the Job List page, which displays information about the job. If the job is a recurring job, then information about all recurrences of this job is displayed. Click **Back** to close the Job List page and return to the Audit Log table.

Click **OK** on the Audit Detail dialog box to close it.

The fields displayed in the Audit Log table are described in [Table 78 on page 604](#).

Table 78: Detailed Audit Logs Information and Audit Log Table Columns

Field	Description
ID	
User Name	Login ID of the user that initiated the task

Table 78: Detailed Audit Logs Information and Audit Log Table Columns (*continued*)

User IP	IP address of the client computer from which the user initiated the task
Domain	Domain from which a user has initiated jobs
Application	Name of the application from which the user initiated the task
Workspace	Name of the workspace from which the user initiated the task
Task	Name of the task that triggered the audit log
Timestamp	UTC time in the database that is mapped to the local time zone of the client computer.
Result	Result of the task that triggered the audit log: <ul style="list-style-type: none"> • Success—Job is completed successfully. • Failure—Job failed and is terminated. • Job Scheduled—Job is scheduled but has not yet started.
Job ID	ID of the job-based task.. Click the job ID to view detailed information about the job. To return to the Audit Log page, click the Back link located at the top left.
Description	Description of the audit log

For both recurring and nonrecurring jobs, such as a database backup operation, the following data described in [Table 79 on page 605](#) is displayed when you click the job ID.

Table 79: Audit Log Details for Recurring and Nonrecurring Jobs

Field	Description
Name	Name of the job
Job ID	Numerical ID of the job
Percent	Percentage of job that is completed
State	State of job execution: <ul style="list-style-type: none"> • SUCCESS—Job is completed successfully. • FAILURE—Job failed and is terminated. • IN PROGRESS—Job is in progress. • CANCELED—Job is canceled by the user.
Job Type	Supported job types. The Junos Space applications determine which job types are supported. In Junos Space 1.4, a recurring job type that is supported is Backup Database.
Summary	Operations executed for the job
Scheduled Start Time	Scheduled start time for the job (specified by a Junos Space user)

Table 79: Audit Log Details for Recurring and Nonrecurring Jobs (*continued*)

Field	Description
Actual Start Time	When the job actually started
End Time	When the job actually ended
Recurrence	Job recurrence interval, start time, and end time

- Related Documentation**
- [Exporting Audit Logs on page 615](#)
 - [Viewing Audit Log Statistics on page 606](#)
 - [Junos Space Audit Logs Overview on page 603](#)
 - [Archiving and Purging Audit Logs on page 611](#)
 - [Backing Up the Junos Space Network Management Platform Database on page 686](#)

Viewing Audit Log Statistics

The Audit Logs workspace statistics page provides two graphs: **Audit Log Statistical Graph** pie chart and the **Top 10 Active Users in 24 Hours** graph. The audit log administrator uses these graphs to monitor the Junos Space Network Management Platform tasks.

The Audit Log Statistical Graph pie chart displays all tasks that are 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 on Ethernet Design. From Network Management Platform 12.1 onward, audit logging is supported on Service Now.

The Top 10 Active Users in 24 hours graph displays the top ten Junos Space Network Management Platform users who performed the most number of tasks over 24 hours. The x-axis represents activities that are performed by a single user. Each active session for that user is represented by a bubble on the x-axis. The 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 displayed on the y-axis.

Viewing the Dynamic Audit Log Statistical Graph

With the Audit Log Statistical Graph, the audit log administrator can view audit logs by selecting both category and time frame. The category—task, user, workspace, or application—determines the statistical graph that is displayed. Each slice in the pie represents a task and its usage percentage. The tasks types are listed in a box at the right of the pie chart. Mouse over a slice of the pie to see the number of times that 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. On the Junos Space Network Management Platform user interface, select **Audit Logs**.

The Audit Logs page appears, which displays Audit Log Statistical Graph and Top 10 Active Users in 24 Hours graph.

2. On the Audit Log Statistical Graph, select a graph category:

- **Task**—Displays all tasks that are performed. Click each task slice to go to the next-level chart that displays users who performed the selected task. For example, when you click the “Login” slice, you can view the login activity (or task) of all users for the selected time frame.

The graph path indicates where you are located in the GUI. In this example, the GUI displays Overview -> Login as the graph path. Click **Overview** to go back to the top-level chart. The task name in the path indicates the currently selected path.

The graph pertaining to a task is displayed with a username or IP address.

- **User Names**—By default, displays all users who performed the specific task. Click a user to go to the inventory page filtered by task, user, and selected time frame.
 - **IP Addresses**—Displays all IP addresses where users performed the specific task. Click an IP address to go to the inventory page filtered by task, IP address, and selected time frame.
 - **User**—Displays all users using the system within the time frame. Ten users are displayed per chart. Click Others to go to the next page. Click the previous page link to go back.
 - **Workspace**—Displays all workspaces accessed 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.
3. Select a time frame in days, weeks, or months to display audit log data in the pie chart for that time period. The default is Days. A time selection description is displayed below the time frame area.
 - **Days**—Displays seven days prior to the selected date. Select single or multiple days. Select multiple days by dragging the cursor along the displayed timeframe.
 - **Weeks**—Displays the past five weeks, from past to most current on the right. Select multiple days by dragging the cursor along the displayed timeframe.

- **Months**—Displays the past 12 months, from past to most current on the right. Select multiple days by dragging the cursor along the displayed timeframe.

The current day, week, or month is highlighted (or selected) by default.

4. Click a slice in the pie chart to view more detailed information. Tasks appear in tabular view by username, user IP address, task, timestamp, results, description, job ID, and level 2 description.

See *Junos Space User Interface Overview* in the *Junos Space User Interface Guide* for more information about manipulating the table data.

5. On the inventory page, double-click an audit log to view more detailed information. For a job-related log entry, click the link in the Job ID column to view a new table that shows the corresponding job information.

In the audit log detail view, if there are multiple affected objects for a log entry, the affected object detail always shows the first object detail. Click any object on the list to change the object detail. If no affected object exists for this log entry, the affected object list is hidden and no object detail is displayed.

6. 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 jobs performed by a user in 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 displays the jobs performed by that user.

Jobs appear by audit log ID, username, user IP address, domain, application, task, timestamp, results, description, and job ID in tabular view. See *Junos Space User Interface Overview* in the *Junos Space User Interface Guide* for more information about manipulating the table data.

Related Documentation

- [Viewing Audit Logs on page 604](#)
- [Junos Space Audit Logs Overview on page 603](#)
- [Archiving and Purging Audit Logs on page 611](#)
- [Exporting Audit Logs on page 615](#)

Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel

You can unzip an audit log *.gz file and open the extracted *.csv file as a spreadsheet in Microsoft Excel. In Microsoft Excel, you can convert the entries in the Timestamp column from Coordinated Universal Time (UTC) to local time.

To convert 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, in (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_2013-07-23_03-45-00_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 - Y/24`
 - Where XX is the cell letter and row number where you want to insert the local time conversion function.
 - Where Y represents the difference in hours between your local time and the UTC time.
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. From the **Category** list, select **Date**.
11. From the **Type** list, 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 5 on page 609](#).

Figure 5: 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	81E07BEDEF597C8CASECCEB14347FA29
3	1900821	0	1.26971E+12	3/27/10 13:14	40264.71815	10.150.113.211	Network Application Platform	Logout	Success	IN
4	1966342	0	1.26971E+12	3/27/10 13:24	40264.72646	10.150.113.211	Network Application Platform	Login	Success	IN
5										

14. If you want to keep the original audit log file, save it with a different filename.

Related Documentation

- [Archiving and Purging Audit Logs on page 611](#)

CHAPTER 63

Archive / Purge

- [Archiving and Purging Audit Logs on page 611](#)

Archiving and Purging Audit Logs

The administrator can archive and then purge all audit logs up to a specified date 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 *yyyy-mm-dd* format, *time* specifies hours, minutes, and seconds, in the *hh-mm-ss* format, 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 Logs from the Database on page 611](#)
- [Archiving Audit Logs to a Remote Server and Purging the Logs from the Database on page 612](#)

Archiving Audit Logs to a Local Server and Purging the Logs from the Database

You can archive audit logs to a local server. A local server is the server that functions as an 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. On the Junos Space Network Management Platform user interface, select **Audit Logs** > **Audit Log** and select the **Archive/Purge Logs** icon. The Archive/Purge Logs dialog box appears.
2. From the **Archive Logs Before** list, 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 specify only a date and time in the past.



NOTE: If you do not select a date and time from the Archive Logs Before list, Junos Space Network Management Platform archives and then purges from the database all logs generated up to the time that you initiated the operation.

3. From the **Archive Mode** list, select **local** to archive the logs locally on the Junos Space server.
4. 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 and 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 and purge operation.



NOTE: The selected time in the scheduler corresponds to the Junos Space server time but uses the local time zone of the client computer.

5. Click **Submit**.

The Audit Log Archive and Purge confirmation dialog box displays the audit log filename 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 and purge operation, click 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 Logs from 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. On the Junos Space Network Management Platform user interface, select **Audit Logs > Audit Log** and select the Archive/Purge Logs icon. The Archive/Purge dialog box appears.
2. From the **Archive Logs Before** list, 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 select only a date and time from the past.



NOTE: If you do not specify a date and time from the Archive Logs Before list, Junos Space Network Management Platform archives and then purges from the database all logs generated up to the time that you initiated the operation.

3. From the **Archive Mode** list, select **remote**.
4. In the **User** field, enter a valid username to access the remote host server.
5. In the **Password** field, enter a valid password to access the remote host server.
6. In the **Confirm Password** field, reenter the password you entered in the previous step.
7. In the **Machine IP** field, enter the IP address of the remote host server.
8. In the **Directory** field, 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 and 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 and purge operation.



NOTE: The selected time in the scheduler corresponds to the Junos Space Network Management Platform server time but uses 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 are copied.

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 and purge operation, click the Job ID link.
13. Click **OK** to close the dialog box.

Related Documentation

- [Junos Space Audit Logs Overview on page 603](#)
- [Viewing Audit Logs on page 604](#)
- [Exporting Audit Logs on page 615](#)

Export

- [Exporting Audit Logs on page 615](#)

Exporting Audit Logs

You can export audit logs without purging them from the system.

To export audit logs, you have three options to select from:

- Export all audit logs.
- Export audit logs filtered by date range.
- Export audit logs as displayed in the Audit Log table. On the Audit Log page, you can filter audit logs by using multiple criteria. The criteria you choose determine which audit log data is exported. The filter determines which records appear in the table, and the records in the table are exported.

The audit logs are exported as CSV files and are not removed from the database when they are exported.

1. On the Junos Space Network Management Platform user interface, select **Audit Logs > Audit Log**.

The Audit Log page appears.

2. Click the **Export Audit Logs** icon. The Export Audit Logs page appears.

3. Perform one of the following actions and click **Export**.

- To export all logs, select **Export all audit logs**.

The Date and Time selectors are disabled when you select this option.

- To export logs within a specific duration, select **Export audit logs filtered by date range**.

The Date and Time widget selectors are enabled when you select this option.

- To export all logs that are currently displayed on the Audit Log page, select **Export audit logs currently displayed in View Audit Logs table**

This is the default selection. For instructions on how to filter audit logs, see “Filter Submenus” in the *Inventory Landing Page* section in the *Junos Space User Interface Guide*.

Your browser’s Download dialog box appears.

4. You can either open the exported file or save it.

**Related
Documentation**

- [Junos Space Audit Logs Overview on page 603](#)
- [Viewing Audit Log Statistics on page 606](#)
- [Archiving and Purging Audit Logs on page 611](#)

PART 12

Administration

- [Overview on page 619](#)
- [Fabric on page 627](#)
- [Managing Databases on page 683](#)
- [Manage Licenses on page 701](#)
- [Manage Applications on page 705](#)
- [Troubleshoot Space on page 735](#)
- [Manage Certificates on page 745](#)
- [Manage Authentication Servers on page 757](#)
- [Manage SMTP Servers on page 775](#)
- [Manage Tags on page 779](#)
- [Manage DMI Schemas on page 803](#)
- [Generate Key on page 817](#)

Overview

- [Junos Space Administrators Overview on page 619](#)
- [Maintenance Mode Overview on page 621](#)
- [Running Applications in Separate Server Instances on page 622](#)

Junos Space Administrators Overview

Juniper Networks® Junos® Space administrators 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 Junos Space Appliances are installed and configured, users created from the Junos Space user interface perform the roles of accessing workspaces and managing applications, users, devices, services, customers, and so forth. Typically, an administrator performs most of the tasks from the Administration workspace. This entire workspace is available only if you are working in the global domain. You can identify the domain that you are currently in from the banner on the Junos Space Network Management Platform user interface. In subdomains, only the tags task is available under the Administration workspace.

[Table 80 on page 619](#) describes Junos Space administrators and Junos Space user interface users and the tasks that they perform.

Table 80: Junos Space Administrators and Junos Space User Interface Users

Junos Space Administrator	Description	Tasks
---------------------------	-------------	-------

Table 80: Junos Space Administrators and Junos Space User Interface Users (*continued*)

CLI administrator	<p>An administrator responsible for setting up and managing the 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 Junos Space appliances, for example: <ul style="list-style-type: none"> • Change the CLI administrator password. • Change network settings, such as: <ul style="list-style-type: none"> • Set DNS servers. • Change IP address of the Junos Space node. • Change static routes. • Change time options. • Expand VM drive size (Junos Space Virtual Appliances only). <p>NOTE: This option is available only if the Junos Space node is running on a virtual machine (VM).</p> <ul style="list-style-type: none"> • Retrieve log files for troubleshooting. • Update the security settings, such as disable firewall or SSH • Debug
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>You can configure the maintenance-mode password is through 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 its 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 the Junos Space Network Management Platform.
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, and so on) available from a workspace on the Junos Space user interface.</p>	<p>For complete information about predefined roles that can be assigned to a Junos Space user, see "Predefined Roles Overview" on page 521.</p>

- Related Documentation**
- [Maintenance Mode Overview on page 621](#)
 - [Role-Based Access Control Overview on page 519](#)
 - [Configuring Users to Manage Objects in Junos Space Overview on page 521](#)

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 shut down 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 goes 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 login page. Users who logged in to Junos Space Network Management Platform before the shutdown and attempt to perform an action on the user interface are also redirected to the maintenance mode login page.

- An authorized Junos Space administrator initiates a Restore operation from the Database Backup and Restore workspace to restore a database.

When a user initiates a Restore operation, Junos Space Network Management Platform prompts the user to type a username 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 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 to type a username 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 operation.

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 is released 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 five minutes during which another administrator can log in.

Maintenance-Mode User Administration

The username for the maintenance-mode administrator is “maintenance.”

You can set the password for the maintenance-mode administrator through the Junos Space system console during the initial installation and configuration of a Junos Space Appliance or Junos Space Virtual Appliance.

A Junos Space administrator connects to a Junos Space Appliance that is already in maintenance mode by using the URL `https://ip-address/maintenance`, where *ip-address* is the Web-access IP address of the Junos Space Appliance.

Related Documentation

- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 692](#)
- [Backing Up the Junos Space Network Management Platform Database on page 686](#)
- [Backing Up and Restoring the Database Overview on page 684](#)

Running Applications in Separate Server Instances

Junos Space enables you to deploy an application to a separate instance within an application server so that you can allocate resources to each application. You can individually shut down an instance without affecting other instances that are running other applications.

Junos Space Release 13.3R1 and later versions run on JBoss EAP 6, which supports the concept of a managed domain. A domain comprises one or more server groups and each server group comprises one or more server instances. A domain is controlled by a domain controller, which ensures that each server is configured according to the management policy of the domain. With this feature, you can deploy each application to a separate server instance, if needed. You can also shut down individual instances without affecting other instances that are running other applications.

Before you install Junos Space Network Management Platform, it is necessary that you set up the infrastructure of server groups and add servers to the server groups so that you can install an application such as Security Designer on a specific server instance. After the setup is ready, add the application from the Junos Space user interface (see [“Adding a Junos Space Application” on page 721](#)).



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

Instructions to set up, start, stop, or remove a server instance are in the following topics:

- [Adding a Server Group on page 623](#)
- [Adding a Server to a Server Group on page 624](#)
- [Starting Servers in a Server Group on page 625](#)
- [Stopping Servers in a Server Group on page 625](#)
- [Removing a Server Group on page 625](#)
- [Moving an Application to a Different Server Group on page 626](#)

Adding a Server Group

A server group comprises one or more server instances that are managed and configured as one. All servers (server instances) of the same server group perform the same tasks because they share the same profile configuration and deployed content.

To add a server group:

1. Launch the management CLI in Linux by typing the following text at the command prompt:
`EAP_HOME/bin/jboss-cli.sh`
2. Type the following text:
`$sh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>
"/server-group=<SERVER_GROUP_NAME>:add(profile=full-ha,socket-binding-group=full-ha-sockets)"`

In this text:

- `DOMAIN_CONTROLLER_HOST` is the hostname of the server that runs Junos Space Network Management Platform.
- `SERVER_GROUP_NAME` is the name of the server group that you want to add.



NOTE: Refer to the JBoss version 6 documentation set for more information about configuring the `profile` and `socket-binding-group` parameters.

The configuration in this topic provides you with full clustering capabilities because you have used the `profile=full-ha` parameter at the command prompt.

For the newly added server group to appear in the Junos Space GUI:

1. From the shell console, enter `/var/cache/jboss/jmp/payloads/`.

2. Navigate to the directory in which you have installed the application. For example, `/var/cache/jboss/jmp/payloads/ICEAAA.xxxx/`.
3. Open the `swindex.txt` file and add the following text:
`IsOnlyDeployedWithPlatform=false`.

Adding a Server to a Server Group

You should add a new server to a server group so that you can run an application separately on this server. However, when you install Junos Space Network Management Platform, by default a **platform** server group is created and all the applications are added to this server group automatically.

To add a server to a server group:

1. Launch the management CLI in Linux by typing the following text at the command prompt:
`EAP_HOME/bin/jboss-cli.sh`
2. Type the following text:
`$sh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>
"/host=<HOSTNAME>//server-config=<SERVER_NAME>:add(auto-start=true,
group=<SERVER_GROUP_NAME>, socket-binding-port-offset=100)"`

In this text:

- `DOMAIN_CONTROLLER_HOST` is the hostname of the server that runs the Junos Space Network Management Platform.
- `HOSTNAME` is defined in `host.xml` in the `/usr/local/jboss/domain/configuration` directory.
- `SERVER_NAME` is the name of the server that you want to add.
- `SERVER_GROUP_NAME` is the name of the server group to which you want to add the new server.



NOTE: Refer to the JBoss version 6 documentation set for more information about configuring the `auto-start` and `socket-binding-port-offset` parameters.



NOTE: After you have successfully added a server to a server group (for example, consider you have added a server group called `firstServerGrp`), log in to the domain controller and perform the following action:
`/server-group= firstServerGrp/jvm=
firstServerGrp/:add(max-heap-size=1024m,max-permgen-size=256m,heap-size=64m)`

Starting Servers in a Server Group

You need to start a server in a server group before you deploy an application to this server instance.

To start a server in a server group:

1. Launch the management CLI in Linux by typing the following text in a command line:
EAP_HOME/bin/jboss-cli.sh

2. Type the following text:

```
$sh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>  
"/server-group=application/:start-servers"
```

In this text, *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.

This command starts all servers in a server group.

To start a specific server, use the following command:

```
$sh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>  
"/host=<HOSTNAME>server-config=<SERVER_NAME>/start(server=<SERVER_NAME>,blocking=false)"
```

Stopping Servers in a Server Group

You may want to stop the servers within a server group when you no longer need them—for example, in situations where no applications are running on these servers.

To stop a server in a server group:

1. Launch the management CLI in Linux by typing the following text in a command line:
EAP_HOME/bin/jboss-cli.sh

2. Type the following text:

```
$sh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>  
"/server-group=application/:stop-servers"
```

In this text, *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.

This command stops all the servers in a server group.

To stop a specific server, use the following command:

```
$sh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>  
"/host=<HOSTNAME>server-config=<SERVER_NAME>/stop(server=<SERVER_NAME>,blocking=false)"
```

Removing a Server Group

You may want to remove a server group when you no longer need it—for example, in situations where no applications are running on these server groups.

To remove a server group:

1. Launch the management CLI in Linux by typing the following text in a command line:
EAP_HOME/bin/jboss-cli.sh

2. Type the following text:

```
$ssh jboss-cli.sh --connect --controller=<DOMAIN_CONTROLLER_HOST>  
"/server-group=<SERVER_GROUP_NAME>:remove"
```

In this text:

- *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.
- *SERVER_GROUP_NAME* is the name of the server group that you want to remove.

Moving an Application to a Different Server Group

You can move an application from the current server group to a different server group, if needed, by using the `moveApplication.pl` script under the `/var/www/cgi-bin` directory.



NOTE: Before moving an application to another server group (for example, to `secondServerGrp`), log in to the domain controller and perform the following action:

```
/server-group= secondServerGrp /jvm=  
secondServerGrp:add(max-heap-size=1024m,max-permgen-size=256m,heap-size=64m)
```

To move an application from the current server group to another server group:

1. From the shell console, enter `/var/www/cgi-bin`.

2. Type the following text:

```
$perl moveApplication.pl -s <SOURCE_SERVER_GROUP> -d  
<DESTINATION_SERVER_GROUP> -a <APPLICATION_NAME>
```

- *SOURCE_SERVER_GROUP* is the name of the server group from which you want to remove the application.
- *DESTINATION_SERVER_GROUP* is the server group that want to move the application to.
- *APPLICATION_NAME* is the name of the application that want to move from the current server group to another server group.

For example, to move the ICEAAA application from `firstServerGrp` to `secondServerGrp`, type the following text:

```
moveApplication.pl -s firstServerGrp -d secondServerGrp -a ICEAAA
```

Related Documentation

- [Adding a Junos Space Application on page 721](#)
- [Uninstalling a Junos Space Application on page 733](#)

CHAPTER 66

Fabric

- [Fabric Management on page 627](#)

Fabric Management

- [Fabric Management Overview on page 627](#)
- [Adding a Node to an Existing Junos Space Fabric on page 635](#)
- [Viewing Nodes in the Fabric on page 637](#)
- [Configuring the Network Settings of a Node in the Junos Space Fabric on page 641](#)
- [Shutting Down or Rebooting a Junos Space Appliance Node From Junos Space on page 646](#)
- [Deleting a Node from the Junos Space Fabric on page 647](#)
- [Replacing a Failed Junos Space Node on page 649](#)
- [Overall System Condition and Fabric Load History Overview on page 649](#)
- [Monitoring Nodes in the Fabric on page 652](#)
- [Creating a System Snapshot on page 679](#)
- [Deleting a System Snapshot on page 681](#)
- [Restoring the System to a Snapshot on page 681](#)

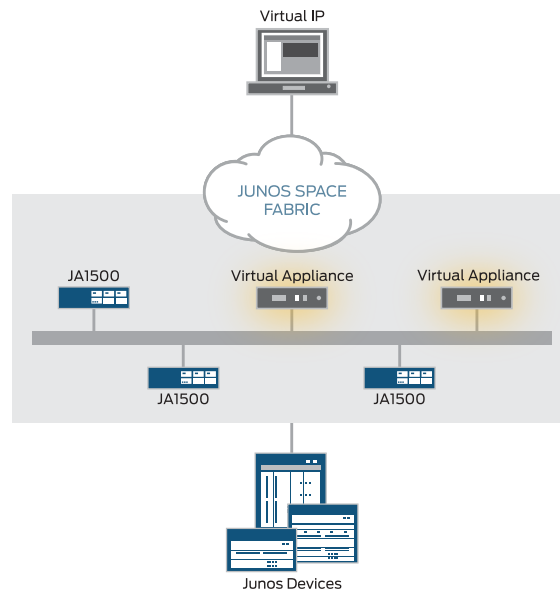
Fabric Management Overview

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 of the Junos Space Network Management Platform GUI. To add, manage, and monitor nodes in the fabric, a fabric administrator (that is, a user with

the System Administrator privileges) connects to a single virtual IP address, as shown in Figure 6 on page 628.

Figure 6: Fabric Nodes



NOTE: All Junos Space Appliances (nodes) in a fabric must be from the same Junos Space Network Management Platform release. For example, a fabric can comprise 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 Junos Space Appliance, all devices in the managed network connect to that Junos Space Appliance. When you install and configure the Junos Space 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 North Bound Interface (NBI) clients
- **Database**—For processing database requests (for create, read, update, and delete operations)
- **Application Logic**—For processing back-end business logic (Junos Space Network Management Platform service requests) and Device Mediation Layer (DML) workload (that is, any interaction between Junos Space and any device, such as device connectivity, device events, and logging events)



NOTE: A fabric that comprises a single node provides no workload balancing and no backup if the Junos Space 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 Junos Space Appliance, Junos Space Network Management Platform automatically creates a fabric with one node. For each additional Junos Space Appliance that you install and configure, you must add a node to logically represent that Junos Space 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 high 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 (for create, read, update, and delete operations) 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.

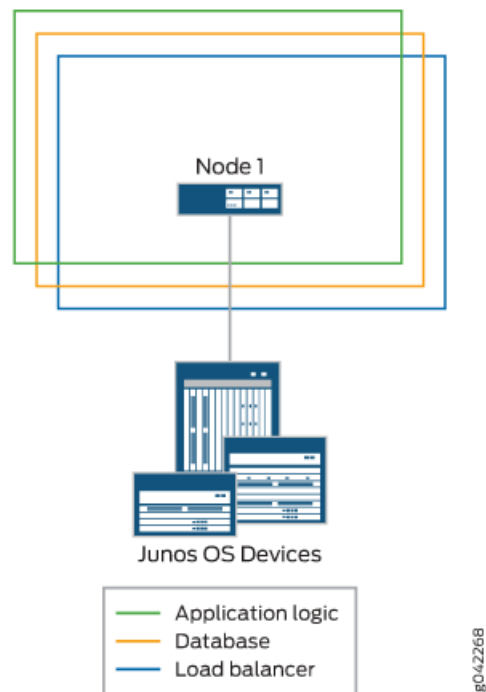
Junos Space Network Management Platform uses the following algorithm to ensure that the number of devices connected to a node does not exceed the threshold limit for each node:

$$\text{Threshold Limit} = \left[\frac{(\text{Number of Devices in Database})}{(\text{Number of Nodes Running})} \right] + 2$$

The following workflow describes how the node functions are enabled across the fabric as nodes are added:

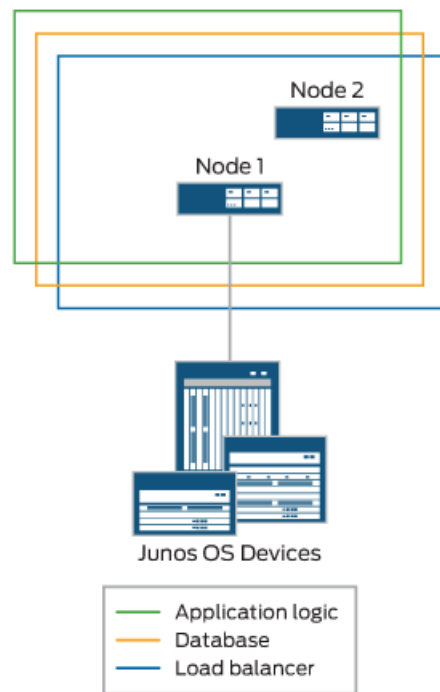
- **Adding the first node**—The load balancer, database, and application logic functions are enabled on the node. Each node function provides both scalability and high availability. [Figure 7 on page 630](#) shows all functions enabled on a fabric comprising one node.

Figure 7: Fabric with One Node



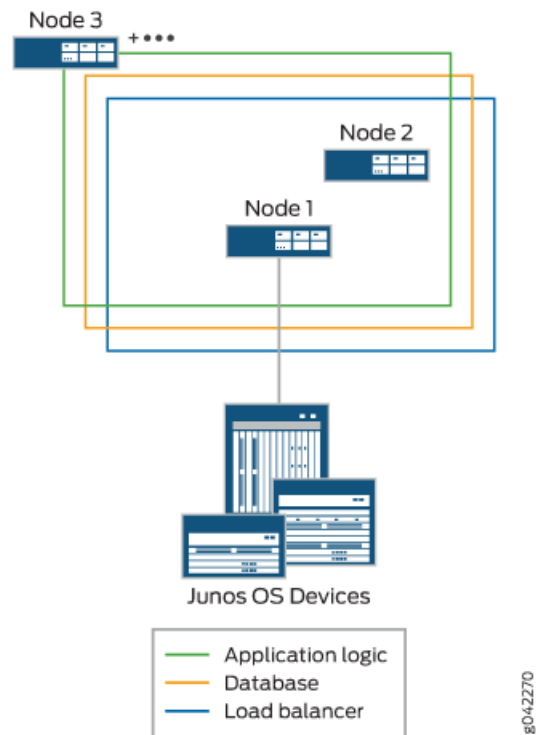
- Adding the second node—When a second node is added to the fabric, the first node functions as the active load-balancer server and active database server, and the second node functions as the standby load-balancer server and standby database server. The load-balancer and application logic node functions provide scalability and high availability. The database node function on the second node provides high availability only. [Figure 8 on page 631](#) shows the functions enabled on a fabric comprising two nodes.

Figure 8: Fabric with Two Nodes



- Adding the 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 9: Fabric with Three Nodes



NOTE: For the third node and each subsequent node added to the fabric, only the application logic functionality is enabled.

Specialized Node Functionality

When you administer a large or complex network, you may want to dedicate specific Junos Space functionality to particular fabric nodes in order to optimize performance. To meet this requirement, Juniper Networks has introduced a node in the Junos Space fabric dedicated solely to fault and performance monitoring (Fault Monitoring and Performance Monitoring node or FMPM node).

When you add the FMPM node to the fabric, the network monitoring functionality is disabled on the Junos Space nodes and is enabled on the FMPM node. All the devices and nodes now send their traps to the newly added FMPM node. This feature provides you with a high performance network monitoring solution for networks with more than 15,000 small devices or a few devices with thousands of interfaces.

You can have a cluster of FMPM nodes hosting a single service, such as the network monitoring functionality. An FMPM team can consist of a maximum of two FMPM nodes. The network monitoring service present in an FMPM team is considered part of the Junos Space Network Management Platform and may be used by one or more applications. Having more than one node in a cluster provides high availability (HA).



NOTE: At the time of installation of a node, you have the option to install the node as a Junos Space node or an FMPM node. Functionality cannot be changed at runtime. You have to reinstall the node to change the functionality.

To add a specialized node:

1. Install the FMPM specialized node (using OVA or Junos Space Network Management Platform ISO) on a virtual machine (VM) or a Junos Space Appliance (JA1500). You use the same Junos Space Network Management Platform image for installing the specialized node. The workflow during the installation has been modified to identify and boot the node as an FMPM node.

For installation instructions, see the following sections in the *Junos® Space JA1500 Appliance User Guide* or the *Junos® Space Virtual Appliance Installation Guide*:

- Configuring an FMPM First Node
- Adding an FMPM node for High Availability



NOTE: The operating system of the node must support and contain sufficient RAM (32 GB is recommended), CPU, and disk space (100 GB is recommended). When you configure the disk space, you might want to allocate slightly more than 100 GB, say 102 or 103 GB to get 100 GB of disk space.

2. Add the specialized node to an existing Junos Space fabric—Junos Space Network Management Platform and other applications use the services provided by this node.

The nodes that are added are deployed into a Junos Space cluster in a similar fashion to a regular application node.



NOTE:

- You can add up to a maximum of two FMPM nodes to an FMPM team.
- The network monitoring service runs on the first FMPM node (primary node). The network monitoring database (PostgreSQL database) is replicated from the primary FMPM node to the standby FMPM node.

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. When the primary FMPM node (usually the first FMPM node) is down or being rebooted, the standby node automatically assumes charge.



NOTE: The functions of the FMPM node:

- When the first FMPM node is up, the network monitoring functionality is enabled on this node and the PostgreSQL database runs on this node.
- When you add a second FMPM node to the fabric, the first node functions as the primary node, and the second node functions as the standby. The second node assumes charge when the primary node (first node) is down.
- A third FMPM node cannot be added.

On a successfully installed FMPM node, you can perform most of the actions that are permitted on a Junos Space node, such as:

- Monitor the FMPM node
- Configure the IP address of the FMPM node (from **Network Management Platform > Fabric > Space Node Settings**)
- Delete the FMPM node

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 the 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 (that is, the Junos Space 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 the active server.

Related Documentation

- [Viewing Nodes in the Fabric on page 637](#)
- [Adding a Node to an Existing Junos Space Fabric on page 635](#)
- [Monitoring Nodes in the Fabric on page 652](#)

Adding a Node to an Existing Junos Space 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 through 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 Junos Space nodes are connected;
- IGMP-Snooping needs to be disabled on the switches to which Junos 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. On the Junos Space Network Management Platform user interface, select **Administration > Fabric** and then click the **Add Fabric Node** icon.

The Add Node to Fabric 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 that are 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.
- In addition, 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 readded to the fabric.

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

The name of the fabric node cannot exceed 32 characters and cannot contain space.

3. In the **IP address** field, enter the IP address of the Junos Space Appliance.



NOTE: This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

4. To add the node as a specialized node, select the **Add as a specialized node** check box.

Enter the login credentials (SSH username and password) of the specialized node. The credentials should be the same as that you specified when you configured the node initially from the command-line interface, at the time of installation.

If the credentials do not match, the add node operation (job) is a failure and Junos Space Network Management Platform displays the following error message on the Job Management workspace:

Please check network credentials

For a specialized node, the add node operation might fail when:

- You provide the VIP address in the **IP address** field instead of the IP address for the eth0 interface
 - You enter the wrong credentials
 - The IP address of the FMPM node is not reachable
 - You add a non-FMPM node as a specialized node
 - You provide a duplicate IP address (that is, you provide an IP address of a Junos Space node or a previously added FMPM node)
5. (Optional) Schedule when you want to add the fabric node:
 - Clear the **Schedule at a later time** check box (the default) to initiate the add operation when you complete step 6 of this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the add operation.



NOTE: The selected time in the scheduler corresponds to the Junos Space server time but is mapped to the local time zone of the client computer.

6. Click **Add** to add the node to the fabric.

The node is added to the fabric and appears on 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 (that is, excluding the FMPM team).

If you have added a specialized node (that is, an FMPM node), the first FMPM node performs the fault and performance monitoring of all the devices and nodes. You can add a maximum of two FMPM nodes. An FMPM team can monitor the nodes that have been added to the Junos Space fabric and also the devices that have been discovered from Junos Space Network Management Platform.

When the first FMPM node is added, Junos Space backs up the network monitoring data from the VIP node and restores it on the FMPM node. The network monitoring functionality is disabled on the Junos Space node and is enabled on the FMPM node. When a second FMPM node is added, the first FMPM node acts as the active PostgreSQL database server and the second node acts as the secondary database server. Only the PostgreSQL database content is continuously replicated from the active server to the standby server. The configuration files that are stored outside of the PostgreSQL database are backed up everyday only at midnight. If you reboot the first node or if the first node is down, the second node automatically takes over the network monitoring functions.

Related Documentation

- [Fabric Management Overview on page 627](#)
- [Viewing Nodes in the Fabric on page 637](#)
- [Overall System Condition and Fabric Load History Overview on page 649](#)

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 637](#)
- [Viewing Fabric Node Details on page 638](#)
- [Performing Fabric Node Actions on page 640](#)

Changing Views

You can display fabric monitoring in 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 title bar of the Fabric page.

Viewing Fabric Node Details

To view detailed runtime and status information for a node:

- Double-click a node in tabular view. The **View Node Detail** page appears.

[Table 81 on page 638](#) describes the node information displayed in each column in the table and from the detailed view.

Table 81: Fields for the Fabric Monitoring Inventory Page

Field	Description
Node name	Logical name assigned to the node 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.
Management IP	IP address for the node
Device Connection IP	IP address for connecting to the device
Status	Connection status for the node <ul style="list-style-type: none"> • UP—Node is connected to the fabric. • DOWN—Node is disconnected from the fabric.
% CPU	Percentage of CPU resource utilized by the node; from 0 to 100% <ul style="list-style-type: none"> • Unknown—Percentage of CPU utilized is unknown, for example, because the node is not connected
% Memory	Percentage of memory resource utilized by the node; from 0 to 100% <ul style="list-style-type: none"> • Unknown—Percentage of memory utilized is unknown, for example, because the node is not connected
% DISK	Percentage of the /var directory utilized by the node; from 0 to 100% <ul style="list-style-type: none"> • Unknown—Percentage of the /var directory utilized by the node is unknown, for example, because the node is not connected

Table 81: Fields for the Fabric Monitoring Inventory Page (*continued*)

Field	Description
App Logic	<p>Application logic function status for the node</p> <ul style="list-style-type: none"> UP—Application logic function is running on the 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)—Configured primary Junos Space node in the fabric FMPM (Master)—The configured primary specialized node in the fabric. FMPM—The configured secondary specialized 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 the 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)—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: The hardware model appears when you double-click a table row for a detailed view of the node.</p> <p>NOTE: The hardware model applies only to a physical Junos Space Appliance.</p>
Software version	<p>Junos Space Network Management Platform release version</p> <p>NOTE: Software version appears when you double-click a table row for a detailed view of the node.</p>
Serial number	<p>The serial number for the Junos Space Appliance</p> <p>NOTE: Serial number appears when you double-click a table row for a detailed view of the node.</p>

Table 81: Fields for the Fabric Monitoring Inventory Page (*continued*)

Field	Description
Cluster Member IPs	IP addresses of the nodes in the fabric
Is Master Node	Indicates whether the node is a master node. <ul style="list-style-type: none"> TRUE—The node is a master node. FALSE—The node is not a master node.
Is VIP Node	Indicates whether the 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—The node is a VIP node. FALSE—The node is not a VIP node.
Virtual Machine IPs	Lists the virtual machine IPs hosted by the node.

For more information about manipulating data on the Fabric inventory page, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

Performing Fabric Node Actions

To perform an action on a fabric node,

1. Select a node by clicking the check box adjacent to the node on the Fabric page.
2. Select an action from the Actions menu or the toolbar icons.

From the Fabric inventory page, you can perform the following actions:

- **Shutdown Node**—Shut down or reboot a fabric node (appliances or virtual machine hosts) when you move it or reconfigure its network settings. See [“Shutting Down or Rebooting a Junos Space Appliance Node From Junos Space” on page 646](#).
- **Delete Fabric Node**—Remove a 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 647](#).

- **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 793](#).
- **View Tags**—View tags applied to a fabric node. See [“Viewing Tags for a Managed Object” on page 794](#).
- **Untag It**—Remove a tag from a fabric node. See [“Untagging Objects” on page 794](#).
- **Clear All Selections**—Clear the selection from all objects selected on the inventory page.

**Related
Documentation**

- [Overall System Condition and Fabric Load History Overview on page 649](#)
- [Fabric Management Overview on page 627](#)
- [Monitoring Nodes in the Fabric on page 652](#)

Configuring the Network Settings of a Node in the Junos Space Fabric

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 setup 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 the Junos Space fabric from one network location to another location, requiring no 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.

You need to restart the nodes to apply the new network settings.

This topic includes the following topics:

- [Network Settings Configuration Guidelines on page 642](#)
- [Changing the VIP Interface in the Same Subnet on page 642](#)
- [Changing the Node Management IP in the Same Subnet on page 642](#)
- [Changing the Default Gateway on page 642](#)
- [Changing the Management IP to a Different Network on page 643](#)
- [Adding the Device Management IP Address on page 643](#)
- [Changing the Device Management IP Address in the Same Subnet on page 644](#)
- [Changing the Device Management IP Address to a Different Network on page 644](#)
- [Deleting a Device Management IP Address on page 644](#)
- [Changing the VIP Interface to a Different Network on page 645](#)

- [Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet on page 645](#)
- [Changing the VIP Interface of a Multiple-Node Fabric to a Different Network on page 645](#)

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 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 **Confirm**.

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 **Confirm**.

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 **Confirm**.

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 IP, subnet mask, and default gateway for the device management interface.
5. Click **OK**.
6. Click **Confirm**.

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 **Confirm**.

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 **Confirm**.

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 **Confirm**.

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 **Confirm**.

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 **Confirm**.

The Shutdown/reboot confirmation dialog box appears.

Changing the VIP Interface of a Multiple-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 multiple-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 **Confirm**.

The Shutdown/reboot confirmation dialog box appears.

**Related
Documentation**

- [Shutting Down or Rebooting a Junos Space Appliance Node From Junos Space on page 646](#)

Shutting Down or Rebooting a Junos Space Appliance 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 from the Fabric page using the steps mentioned below. 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 in to the node using the CLI. The message appears on UNIX shell).

If you do not enter any text, console users see either **Junos Space shutdown** or **Junos Space reboot** on the shell.

6. Click **Confirm**.

The node in the fabric is shut down or rebooted.



NOTE: If you are shutting down a node after a change of IP address, it is recommended that you reboot all nodes for the changes to take effect.

**Related
Documentation**

- [Fabric Management Overview on page 627](#)
- [Deleting a Node from the Junos Space Fabric on page 647](#)
- [Viewing Nodes in the Fabric on page 637](#)

Deleting a Node from the Junos Space Fabric

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 reimage it. Then, you can add it to the fabric by selecting **Administration > Fabric** and the **Add Fabric Node** icon.



NOTE: You cannot delete a primary FMPM node (master FMPM node) if a secondary FMPM node exists. Junos Space Network Management Platform displays the following error message:

Primary FMPM node cannot be deleted if secondary FMPM node exist.

The workaround to delete the primary FMPM node is to perform one of the following actions:

- Shut down the primary FMPM node and then delete this node.
- Reboot the primary FMPM node and then delete this node. When you reboot this node, automatic failover happens and the secondary node takes charge as the primary FMPM node.

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 another node 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 no node exists to which you can transfer that role, high availability does not occur.

When you delete a fabric node, Junos Space Network Management Platform performs the following tasks:

- Removes references to the host name and IP address of that node from the remaining nodes
- Stops database replication on both the deleted node and the backup database node
- Makes the database backup copy in that node unavailable for the remaining nodes to restore the database from the backup copy
- Copies the database to the new database node
- Shuts down all services that interact with other nodes

When an FMPM node is deleted, as part of the deletion job, the FMPM data from the FMPM node is backed up and restored on the Junos Space node, and then the FMPM node is deleted from the Junos Space fabric. Thereafter, the network monitoring service is enabled on the Junos Space node.

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**.
2. Select the node that you want to delete, and click the **Delete Fabric Node** icon.
3. 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 that 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 assume that role.
4. In the **Delete** dialog box, select the node that you want to delete.
5. Click **Delete**.

Node deletion is scheduled as a job immediately after you click **Delete**. Deleting a node generates an audit log entry. The **Delete Fabric Node Job Information** dialog box appears.

6. In the **Delete Fabric Node Job Information** dialog box, click the **Job ID** link.

The Job Management inventory landing page appears displaying this job. From this page, you can verify and monitor information about the node you are deleting, such as the job type, job ID, percentage of task completion, job state, scheduled start and end times, username, a brief job summary, and so on.



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 627](#)
- [Viewing Nodes in the Fabric on page 637](#)
- [Adding a Node to an Existing Junos Space Fabric on page 635](#)
- [Replacing a Failed Junos Space Node on page 649](#)

Replacing a Failed Junos Space Node

This topic provides information about how to replace a failed Junos Space node with a new one. Typically, the status of a failed node is shown as **DOWN** on the Administration > Fabric inventory landing page.

1. Delete the failed node on the **Administration > Fabric** inventory landing page by using the **Delete Fabric Node** task. For detailed instructions for deleting a node from a Junos Space cluster, see [“Deleting a Node from the Junos Space Fabric” on page 647](#).

When you delete a node, a job is triggered. To confirm whether the node is deleted successfully, check the status of this job on the Job Management page.

2. Install, configure, and add the new node to the existing Junos Space cluster by following the instructions in “Adding a Junos Space Virtual Appliance to an Existing Cluster” in the *Junos Space Virtual Appliance* guide.
3. On the Junos Space Network Management Platform user interface, add the newly installed node to the existing Junos Space cluster by using the **Administration > Fabric > Add Fabric Node** task. For detailed instructions about adding a node to a Junos Space cluster, see [“Adding a Node to an Existing Junos Space Fabric” on page 635](#).

When you add a node, a job is triggered. To confirm whether the node is added successfully to the existing Junos Space cluster, check the status of this job on the Job Management page. If the job is a success, then the newly added Junos Space node appears on the **Administration > Fabric** inventory landing page.

Related Documentation

- [Fabric Management Overview on page 627](#)
- [Overall System Condition and Fabric Load History Overview on page 649](#)

Overall System Condition and Fabric Load History Overview

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.

Overall System Condition

To calculate the overall Junos Space system condition, Junos Space Network Management Platform uses a formula 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 the 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 that are running, and then applies the following formula to determine the overall Junos Space system condition:

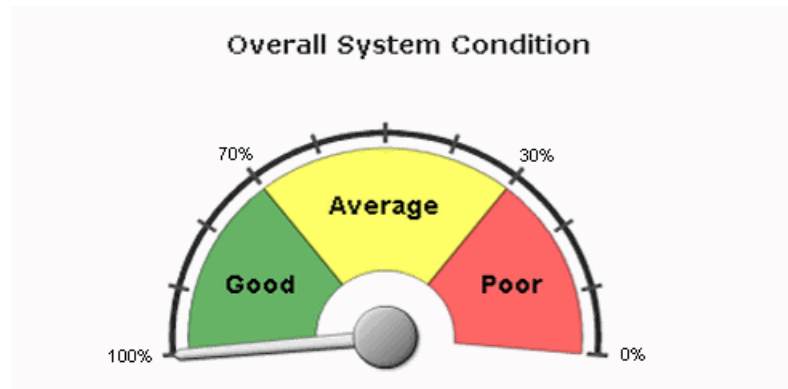
$$\text{Overall System Condition} = [(\text{Number of Nodes Running}) / (\text{Number of Nodes in Fabric})] \\ * [(\text{Number of Nodes Running Load_Balancing Process}) / (\text{Number of Nodes enabled for Load Balancing})] * [(\text{Number of Nodes Running Database-Server Process}) / (\text{Number of Nodes Enabled As Database Server})] * [(\text{Number of Nodes Running Application-Logic Process}) / (\text{Number of Nodes Enabled for Application Logic})]$$

Using the values in the preceding examples for cluster health and node-function health, the overall Junos Space 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%) on the basis of the value that the formula returns.

Figure 10: Overall System Condition Gauge



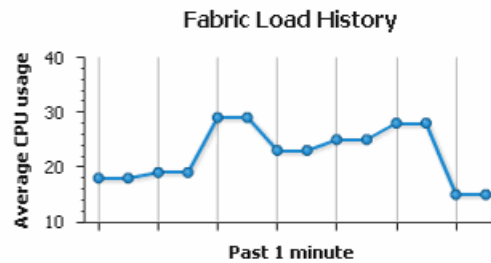
The overall system health indicates 0% (Poor) when any one of the following conditions is detected:

- 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 History

The Fabric Load History chart displays the average CPU usage across all nodes that are running in the fabric.

Figure 11: Fabric Load History Chart



Junos Space Network Management Platform uses the following formula to determine the fabric load:

$$\text{Fabric Load} = (\text{Total CPU Usage for All Nodes Running}) / (\text{Number of Nodes Running})$$

For example, for 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.

$$\text{Fabric Load} = (80\% + 30\% + 10\%) / 3$$

$$\text{Fabric Load} = 120\% / 3$$

$$\text{Fabric Load} = 40\%$$

To view the average CPU usage at a specific data point, mouse over the data point of interest.

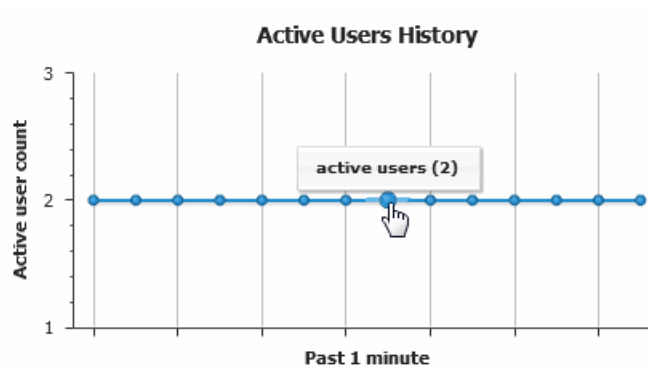
To obtain details about the status of the fabric, click any data point in the graph. The Fabric dialog box appears and shows detailed status for each node in the fabric. Status information includes CPU, disk, and memory usage and indicates up or down status for each node function enabled on the node.

Active Users History

The Active Users History chart displays the number of active users in the past one minute.

To know the users that are currently active, you can click a bubble on the Active Users History chart, which takes you to the Role Based Access Control > User Accounts inventory landing page (ILP). This ILP displays the active users that are currently logged in. If you need more information about the sessions of the active users, such as the IP address from which a user has logged in, the session duration, and so on, navigate to the User Sessions ILP (**Role Based Access Control > User Sessions**).

Figure 12: Active Users History Chart



- Related Documentation**
- [Fabric Management Overview on page 627](#)
 - [Configuring the Network Settings of a Node in the Junos Space Fabric on page 641](#)
 - [Monitoring Nodes in the Fabric on page 652](#)

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 Junos Space to obtain information about the logical components of the nodes using an object identifier (OID) in SNMP v1 and v2, or v3 as a user. The response is provided by the Junos Space SNMP agent. The network monitoring functionality displays the polled data in the Network Monitoring workspace.

[Table 82 on page 652](#) shows the monitoring settings, as well as relevant details.

Table 82: Logical Component Monitoring

Setting	Explanation	Recommended Settings	Default Value	Comments
Enable SNMP over TCP	Enables SNMP communication over TCP	Unselected	Unselected	By default, SNMP communication occurs over UDP.
Monitor Web Service	Includes monitoring the performance of the Junos Space GUI	Selected	Selected	
Monitor All Disks	Includes all disks on the current Junos Space server	Unselected	Unselected	All disks, or specify partition

Table 82: Logical Component Monitoring (*continued*)

Setting	Explanation	Recommended Settings	Default Value	Comments
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	
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 654](#)
- [Starting SNMP Monitoring on Fabric Nodes on page 675](#)

- [Stopping SNMP Monitoring on Fabric Nodes on page 676](#)
- [Restarting SNMP Monitoring on Fabric Nodes on page 676](#)
- [Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node on page 677](#)
- [Adding a Third-Party SNMP V3 Manager on a Fabric Node on page 677](#)
- [Deleting a Third-Party SNMP Manager from a Fabric Node on page 678](#)

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 82 on page 652](#) 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 83 on page 655](#) shows the configuration parameters for monitoring disk usage.

Table 83: SNMP Configuration Parameters: Monitoring Disk Usage

Monitoring Disk Usage

Table 83: 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 13 on page 656](#) is generated.

Figure 13: Disk Usage Threshold Is Normal

	406	space-000c29d796f5	1	3/27/14 12:25:51 [<] [>]	Disk usage is normal.
--	-----	--------------------	---	--	-----------------------

[Figure 14 on page 656](#) shows the OID details for the trap generated when disk usage is normal.

Figure 14: 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	OID	1.3.6.1.4.1.2021.9.1.100.1
mib-2.88.2.1.5.0	Integer	0
diskPath.1	String	/
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	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 15 on page 656](#) is generated.

Figure 15: 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 16 on page 656](#) shows the OID details for the trap generated when disk usage exceeds the configured threshold.

Figure 16: Trap Details When Disk Usage Exceeds Configured Threshold

Table 83: SNMP Configuration Parameters: Monitoring Disk Usage (*continued*)

Monitoring Disk Usage

Trap Details		
Request ID	1141303069	
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	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"/>		

Trap Details		
Request ID	1141303069	
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	Disk space usage 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	1.3.6.1.4.1.2021.9.1.100.1
1.3.6.1.2.1.88.2.1.5.0	Integer	1
1.3.6.1.4.1.2021.9.1.2.1	String	/
1.3.6.1.4.1.2021.9.1.101.1	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 84 on page 658 shows the configuration parameters for monitoring the CPU load average.

Table 84: SNMP Configuration Parameters: Monitoring the CPU Load Average

Monitoring the CPU Load Average (System Load)

Table 84: 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 17 on page 659 is generated:

Figure 17: 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 18 on page 659 shows the OID details for the trap generated when the CPU load is normal.

Figure 18: 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	OID	1.3.6.1.4.1.2021.10.1.100.3
laNames.3	Integer	0
laErrorMessage.3	String	Load-15

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	OID	1.3.6.1.4.1.2021.10.1.100.3
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 19 on page 659 shows the traps generated when the 15 minute, 5 minute, or 1 minute CPU Load Average threshold is exceeded.

Figure 19: 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 20 on page 659 shows the OID details for the trap generated when the CPU load 5 minute average exceeds the threshold.

Figure 20: Trap Details When CPU Load 5 Minute Average Exceeds Threshold

Table 84: 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 >>

Table 85 on page 661 shows monitoring processes for the Junos Space Network Management Platform.


Table 85: SNMP Configuration Parameters: Monitoring Processes

Monitoring Processes

Parameter: Node Management Agent (NMA)

When the NMA process is up, the trap shown in [Figure 21 on page 661](#) is generated:

Figure 21: NMA Is Up

	384	space-000c29d796f5	1	3/27/14 12:10:05 [<] [>]	Process NMA started.
---	-----	--------------------	---	--------------------------	----------------------

[Figure 22 on page 661](#) shows the OID details for the trap generated when the NMA process is up.

Figure 22: Trap Details When NMA Is Up

Trap Details

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 >>

Trap Details

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 23 on page 661](#) is generated:

Figure 23: NMA is Down

	382	space-000c29d796f5	1	3/27/14 12:09:25 [<] [>]	Process NMA stopped.
---	-----	--------------------	---	--------------------------	----------------------

[Figure 24 on page 661](#) shows the OID details for the trap generated when the NMA process is down.

Figure 24: Trap Details When NMA is Down

Trap Details

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 >>

Trap Details

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 85: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Webproxy

When the WebProxy process is up, the trap shown in Figure 25 on page 662 is generated:

Figure 25: WebProxy Is Up

<input type="checkbox"/>	390	space-000c29d796f5	1	3/27/14 12:12:55 [<] [>]	Process WebProxy started.
--------------------------	-----	--------------------	---	--	---------------------------

Figure 26 on page 662 shows the OID details for the trap generated when the WebProxy process is up.

Figure 26: 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	String		1.3.6.1.2.1.88.2.1.5.0	String	
extNames.1	Integer	102	1.3.6.1.4.1.2021.8.1.100.1	Integer	1.3.6.1.4.1.2021.8.1.100.1
extOutput.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 27 on page 662 is generated:

Figure 27: WebProxy Is Down

<input type="checkbox"/>	386	space-000c29d796f5	1	3/27/14 12:12:24 [<] [>]	Process WebProxy stopped.
--------------------------	-----	--------------------	---	--	---------------------------

Figure 28 on page 662 shows the OID details for the trap generated when the WebProxy is down.

Figure 28: 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	String		1.3.6.1.2.1.88.2.1.5.0	String	
extNames.1	Integer	101	1.3.6.1.4.1.2021.8.1.100.1	Integer	1.3.6.1.4.1.2021.8.1.100.1
extOutput.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 85: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: JBoss

When the JBoss process is up, the trap shown in [Figure 29](#) on page 663 is generated:

Figure 29: JBoss Is Up

	394	space-000c29d796f5	1	3/27/14 12:14:46 [<] [>]	Process Jboss started.
---	-----	--------------------	---	--------------------------	------------------------

Figure 30 on page 663 shows the OID details for the trap generated when the JBoss process is up.

Figure 30: 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 31](#) on page 663 is generated:

Figure 31: JBoss Is Down


	391	space-000c29d796f5	1	3/27/14 12:13:01 [<] [>]	Process Jboss stopped.
---	-----	--------------------	---	--------------------------	------------------------

Figure 32 on page 663 shows the OID details for the trap generated when JBoss is down.

Figure 32: 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 85: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Mysql

When the Mysql process is up, the trap shown in Figure 33 on page 664 is generated:

Figure 33: Mysql Is Up

<input type="checkbox"/>	392	space-000c29d796f5	1	3/27/14 12:13:07 [<] [>]	Process Mysql started.
--------------------------	-----	--------------------	---	--------------------------	------------------------

Figure 34 on page 664 shows the OID details for the trap generated when the Mysql process is up.

Figure 34: Trap Details When Mysql Is Up

Trap Details

Request ID1861140036

Error Index0

Error Status0

Communitypublic

Ip Address10.205.56.39

Trap TypeSNMPv2c

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 >>

Trap Details

Request ID1861140036

Error Index0

Error Status0

Communitypublic

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: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 35 on page 664 is generated:

Figure 35: Mysql Is Down

<input type="checkbox"/>	398	space-000c29d796f5	1	3/27/14 12:21:44 [<] [>]	Process Mysql stopped.
--------------------------	-----	--------------------	---	--------------------------	------------------------

Figure 36 on page 664 shows the OID details for the trap generated when the Mysql process is down.

Figure 36: Trap Details When Mysql Is Down

Trap Details

Request ID737121741

Communitypublic

Error Index0

Error Status0

Ip Address10.205.56.39

Trap TypeSNMPv2c

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 >>

Trap Details

Request ID737121741

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: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 85: SNMP Configuration Parameters: Monitoring Processes (*continued*)

Monitoring Processes

Parameter: Postgresql

When the Postgresql process is up, the trap shown in Figure 37 on page 665 is generated:

Figure 37: Postgresql Is Up

<input type="checkbox"/>	393	space-000c29d796f5	1	3/27/14 12:13:48 [<] [>]	Process Postgresql started.
--------------------------	-----	--------------------	---	--------------------------	-----------------------------

Figure 38 on page 665 shows the OID details for the trap generated when the Postgresql process is up.

Figure 38: Trap Details When Postgresql Is Up

Trap Details

Request ID1861140052

Communitypublic

Ip Address10.205.56.39

Error Index0

Error Status0

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

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: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 39 on page 665 is generated:

Figure 39: Postgresql Is Down

<input type="checkbox"/>	389	space-000c29d796f5	1	3/27/14 12:12:53 [<] [>]	Process Postgresql stopped.
--------------------------	-----	--------------------	---	--------------------------	-----------------------------

Figure 40 on page 665 shows the OID details for the trap generated when the Postgresql process is up.

Figure 40: 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 85: 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 41 on page 666 is generated:

Figure 41: Swap Memory Usage Is Normal

<input type="checkbox"/>	405	space-000c29d796f5	2	3/27/14 12:28:43 [<] [>]	Swap memory usage is normal.
--------------------------	-----	--------------------	---	--------------------------	------------------------------

Figure 42 on page 666 shows the OID details for the trap generated when swap memory usage is normal.

Figure 42: Trap Details When Swap Memory Is Normal

Trap Details			Trap Details		
Request ID 1861140788			Request ID 1861140788		
Community public			Community public		
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:00.11s	1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.11s
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	Swap memory clear	1.3.6.1.2.1.88.2.1.1.0	String	Swap memory clear
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	1.3.6.1.4.1.2021.4.100.0	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.4.100.0
mib-2.88.2.1.5.0	Integer	0	1.3.6.1.2.1.88.2.1.5.0	Integer	0
memErrorName.0	String	swap	1.3.6.1.4.1.2021.4.2.0	String	swap
memSwapErrorMsg.0	String		1.3.6.1.4.1.2021.4.101.0	String	
Close Show Raw << prev next >>			Close Show Raw << prev next >>		

When the free swap memory is less than the upper threshold limit, the trap shown in Figure 43 on page 666 is generated:

Figure 43: 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 44 on page 666 shows the OID details for the trap generated when swap memory usage is exceeds upper limit.

Figure 44: Trap Details When Swap Memory Usage Exceeds Upper Limit

Trap Details			Trap Details		
Request ID 1314711189			Request ID 1314711189		
Community public			Community public		
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:00.10s	1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:01m:00.10s
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	Swap memory trigger	1.3.6.1.2.1.88.2.1.1.0	String	Swap memory trigger
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	1.3.6.1.4.1.2021.4.100.0	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.4.100.0
mib-2.88.2.1.5.0	Integer	1	1.3.6.1.2.1.88.2.1.5.0	Integer	1
memErrorName.0	String	swap	1.3.6.1.4.1.2021.4.2.0	String	swap
memSwapErrorMsg.0	String	Running out of swap space (200630368)	1.3.6.1.4.1.2021.4.101.0	String	Running out of swap space (200630368)
Close Show Raw << prev next >>			Close Show Raw << prev next >>		

Table 86 on page 667 shows the configuration parameters for monitoring Junos Space Network Management Platform hardware.

Table 86: SNMP Configuration Parameters: Monitoring Linux Hardware

Monitoring Linux Hardware

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.

Table 86: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

Table 86: 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 45 on page 669](#) is generated:

Figure 45: CPU Fan Speed Normal

	41	space-0256102011000007	1	3/27/14 12:44:58 [<] [>]	CPU fan is normal.
---	----	------------------------	---	--------------------------	--------------------

[Figure 46 on page 669](#) shows the OID details for the trap generated when CPU fan speed is normal.

Figure 46: Trap Details When CPU Fan Speed Is Normal

Trap Details		
Request ID: 1861140860		
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
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
<div> Close Show Row << prev next >> </div>		

When the CPU fan speed is less than the configured threshold (minimum fan speed), the trap shown in [Figure 47 on page 669](#) is generated:

Figure 47: 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 48 on page 669](#) shows the OID details for the trap generated when CPU fan speed lower than the configured threshold.

Figure 48: Trap Details When CPU Fan Speed Is Below the Configured Threshold

Table 86: 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 86: 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 49 on page 671 is generated:

Figure 49: CPU Voltage Normal

42	space-0256102011000007	1	3/27/14 12:44:58 [<] [>]	CPU voltage is normal.
----	------------------------	---	--------------------------	------------------------

Figure 50 on page 671 shows the OID details for the trap generated when CPU voltage is normal.

Figure 50: 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
mib-2.88.2.1.1.0	String	CPU voltage 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	1.3.6.1.4.1.2021.13.16.4.1.3.2
mib-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 51 on page 671 is generated:

Figure 51: CPU Voltage Is Lower Than Configured Threshold

60	space-0256102011000007	1	3/27/14 12:58:20 [<] [>]	CPU voltage too low (mV):3328.
----	------------------------	---	--------------------------	--------------------------------

Figure 52 on page 671 shows the OID details for the trap generated when CPU voltage is lower than the configured threshold.

Figure 52: 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
mib-2.88.2.1.1.0	String	CPU voltage 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	1.3.6.1.4.1.2021.13.16.4.1.3.2
mib-2.88.2.1.5.0	Gauge	3312

Buttons at the bottom include 'Close', 'Show Raw', '<< prev', and 'next >>'.

Table 86: 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 53 on page 672 is generated:

Figure 53: CPU Temperature Normal

<input type="checkbox"/>	260	space-0256042012000014	4	3/28/14 12:33:16 [<] [>]	CPU temperature is normal.
--------------------------	-----	------------------------	---	--------------------------	----------------------------

Figure 54 on page 672 shows the OID details for the trap generated when CPU temperature is normal.

Figure 54: Trap Details When CPU Temperature Is Normal

Trap Details

Request ID

737109630

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:00.12s
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	OID	1.3.6.1.4.1.2021.13.16.2.1.3.2
mib-2.88.2.1.5.0	Gauge	47500

Close

Show Raw

<< prev

next >>

Trap Details

Request ID

737109630

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:00.12s
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	OID	1.3.6.1.4.1.2021.13.16.2.1.3.2
1.3.6.1.2.1.88.2.1.5.0	Gauge	47500

Close

Show Raw

<< prev

next >>

When the CPU temperature exceeds the configured threshold, the trap shown in Figure 55 on page 672 is generated:

Figure 55: 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 56 on page 672 shows the OID details for the trap generated when CPU temperature is higher than the configured threshold.

Figure 56: Trap Details When CPU Temperature Exceeds The Configured Threshold

Trap Details

Request ID

1861140855

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:00.12s
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	OID	1.3.6.1.4.1.2021.13.16.2.1.3.2
mib-2.88.2.1.5.0	Gauge	47500

Close

Show Raw

<< prev

next >>

Trap Details

Request ID

1861140855

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:00.12s
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	OID	1.3.6.1.4.1.2021.13.16.2.1.3.2
1.3.6.1.2.1.88.2.1.5.0	Gauge	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 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 57 on page 674 shows the OID details for the trap generated when Junos Space node is down.

Figure 57: Trap Details Junos Space Node Is Down

OID	Type	Value
sysUpTime.0	TimeTick	0 days 07h 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 58 on page 674 shows the OID details for the trap generated when Junos Space node is up.

Figure 58: Trap Details Junos Space Node Is Up

OID	Type	Value
sysUpTime.0	TimeTick	0 days 07h 12m 37.70s
snmpTrapOID.0	OID	1.3.6.1.4.1.2536.1.3.1.1.1
jnxSpaceNodeIP	IpAddress	10.205.55.77

- Delete Junos Space Node

Figure 59 on page 674 shows the OID details for the trap generated when Junos Space node is deleted.

Figure 59: Trap Details Junos Space Node Is Deleted

The image shows two identical screenshots of the 'Trap Details' dialog box. The dialog has a blue header and a light beige body. It contains the following fields:

- Request ID:** 711137087
- Community:** JUNIPER
- Error Index:** 0
- IP Address:** 10.205.96.138
- Error Status:** 0
- Trap Type:** SNMPv2c

Below these fields is a table titled 'Variable Bindings' with three columns: DID, Type, and Value.

DID	Type	Value
sysUpTime.0	TimeTick	0 days 07h20m44.75s
snmpTrapOID.0	OID	486spacePlatformTraps
mSpaceNodeIP	IPAddress	10.205.96.77
mSpaceObjectState	String	Space node removed successful

At the bottom of the dialog are buttons for 'Close', 'Show Raw', '<< prev', and 'next >>'.

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 Junos Space node is represented as **space-*<number>***.

Figure 60 on page 676 shows a sample view of network monitoring details for the selected fabric node.

Figure 60: Network Monitoring Details for the Selected Fabric Node

SNMP 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)	Overall	94.751%
10.205.56.40	ICMP	92.126%
	SNMP	100.000%
10.205.57.40	Overall	84.252%
	ICMP	100.000%

Node Interfaces

IP Address	IP Host Name	ifIndex	Managed
10.205.56.40	10.205.56.40	M	M
10.205.57.40	10.205.57.40	2	M

General (Status: Active)

Surveillance Category Memberships (Edit)

Notification

You: Outstanding: (Check)
You: Acknowledged: (Check)

Recent Events

Event ID	Time	Severity	Description
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'
72351	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 **Network Management 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 649](#)
- [Fabric Management Overview on page 627](#)
- [Viewing Nodes in the Fabric on page 637](#)

Creating a System Snapshot

You can use the System Snapshot feature to create a snapshot of the system state and roll back 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 fabricwide operation that maintains consistency across all nodes in the fabric.

Typically, you 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 (for example, adding a node to the Junos Space fabric) that have the potential to precipitate the system into an undesirable state. You can delete the snapshot after you have verified that these actions were performed successfully.

System Snapshot is currently supported on a Junos Space fabric that consists of only Junos Space Virtual Machine (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 Junos Space Network Management Platform is 300 GB. The maximum size that a snapshot can occupy for Junos Space Network Management Platform migrated from releases prior to 11.3 is 43 GB. On the Real Appliance (such as JA 1500), the snapshot becomes invalid if it has been kept for a long time because usage of the snapshot volume disk space increases as write operations continue. When the usage reaches the maximum size of snapshot volume, the snapshot is 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 or CD to Junos Space Appliance, and reboot to set USB or CD as the first boot option.
2. Reboot the Junos Space appliance, and select the **rescue-serial** mode while booting.
3. Follow the on-screen steps and select **Skip** when asked whether you want to find an existing Junos Space installation and mount to `mnt/sysimage`.
4. When 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** field.
4. Enter the comments in the **Comment** field.
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 workspace.

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 Elastic Sky X (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 is true:

- There is insufficient disk space on the ESX servers.
- One of the ESX servers has been incorrectly configured.
- One of the nodes is down.
- The fabric consists 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 681](#)
- [Restoring the System to a Snapshot on page 681](#)

Deleting a System Snapshot

To delete a system snapshot:

1. Select **Administration > Fabric**. Click 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 workspace.



NOTE: You may not be able to delete a snapshot of the system state if any of the following conditions is true:

- One of the ESX servers is incorrectly configured.
- The fabric consists of both Junos Space VM and Junos Space Appliance.
- The snapshot does not exist.

Related Documentation

- [Creating a System Snapshot on page 679](#)
- [Restoring the System to a Snapshot on page 681](#)

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**. Click the **System Snapshot** icon.
2. Click **Restore**.
3. Click **OK**.
4. Log in to the ESX servers and power on the VM after a few minutes.



NOTE: If the Junos Space GUI is not accessible on a VM, you can restore the fabric by shutting down every node in the fabric and logging in to ESX servers where the VM is located.

To restore a system snapshot when using a Junos Space Appliance:

1. Select **Administration** > **Fabric**. Click 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 is 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 679](#)
 - [Deleting a System Snapshot on page 681](#)

CHAPTER 67

Managing Databases

- [Backing Up and Restoring the Database Overview on page 684](#)
- [Backing Up the Junos Space Network Management Platform Database on page 686](#)
- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 692](#)
- [Viewing Database Backup Files on page 696](#)
- [Deleting Junos Space Network Management Platform Database Backup Files on page 698](#)
- [Viewing Database Backup Job Recurrence on page 699](#)

Backing Up and Restoring the Database Overview

As system administrator, you can perform Junos Space Network Management Platform database backup, restore, and delete operations. 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 (Return Material Authorization (RMA)) and restore the configuration that existed 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 operation from the Administration > Database Backup and Restore workspace.

When you initiate a backup operation, 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 by clearing the **Network Monitoring** check box from the Database Backup page (Administration > Database Backup and Restore > Database Backup). 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.



NOTE: Junos Space Network Management Platform allows you to perform backup and restore operations even when the network-monitoring service is turned off.

In Junos Space Release 13.1 and earlier, a local backup operation saves the backup file of the Junos Space database to a specific folder (`/var/cache/jboss/backup`) on the active node. As an administrator, you may want the backup files to exist on both the primary and secondary nodes so that when one of the nodes crashes you can restore the system from the backup file saved on the other node. In this release, backup is initiated on the secondary node and the backup file is saved to the default location (`/var/cache/jboss/backup`) on the secondary node. If the backup operation is successful, then the backup file is synchronized with (copied to) the primary node. The following are the advantages:

- The backup file is present on both the primary and secondary nodes due to which you can restore the system if one of the nodes crashes or is corrupted.
- System performance of the primary node is not impacted because the backup operation is initiated on the secondary node.



NOTE: For disaster recovery, different, additional database backup and restore provisions must be made.

Restore the Junos Space Network Management Platform database if any of the following

issues 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 is 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.

In a multinode setup, the same backup file can exist on both the primary and secondary nodes. In such cases, when you choose to restore a system from a local backup file, Junos Space Network Management Platform randomly chooses a backup file from one of the nodes to restore the system.

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 backup operations. All jobs that are completed before the start of the backup operation are captured in the database backup file.

During a backup operation, 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 operation. When the administrator performs a local backup operation, 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 Protocol (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 operation 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 686](#).

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 its previous state. The administrator can restore the database through the Administration > Database Backup and Restore workspace (see [“Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface” on page 692](#)).

The restore database operation is performed 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 Network Management Platform.



NOTE: After the Junos Space Network Management Platform database is restored, the Security Design database must be manually reindexed. For more information about Security Design, see the Security Design documentation.

**Related
Documentation**

- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 692](#)
- [Backing Up the Junos Space Network Management Platform Database on page 686](#)
- [Maintenance Mode Overview on page 621](#)

Backing Up the Junos Space Network Management Platform 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. As an administrator, you should be able to back up all system data, which includes all databases (MySQL and network monitoring data) and configuration files, and you should be able to save the backup file on both the primary and secondary nodes. This fallback system allows you to restore the system even if one of the database nodes crashes. Typically, 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 operation to copy the backup file to the default directory `/var/cache/jboss/backup`. You perform a remote backup operation to copy the backup file to remote network hosts or media.



NOTE: Before you perform a local backup operation, be aware of the following points. If your fabric consists of:

- One node, then the backup file is saved on the primary node.
- Two or more nodes, then the backup operation is initiated only from the secondary node and the backup file is saved to the `/var/cache/jboss/backup` location on the secondary node.

If the backup operation is successful, then the backup file is synchronized with (copied to) the primary node. Then both primary and secondary nodes have the same backup file. However, if the backup operation fails on the secondary node (for reasons such as insufficient space), then the backup operation is performed on the primary node.



NOTE:

- In a fabric comprising two or more nodes, only the first two nodes (primary and secondary nodes) are considered database nodes and therefore contain database backup files. Only the application logic functionality is enabled on the remaining nodes.
- The database backups are stored on the Junos Space nodes. The backups stored on these nodes contain MySQL data (from the Junos Space nodes) and network monitoring data (from the specialized nodes)

When you back up the Junos Space Network Management Platform database, an audit log entry is automatically generated. From the Audit Log inventory page, you can filter the data on the Task column by using the “Database Backup” keyword to view details about the database backup operations that were performed.

This topic includes the following tasks:

- [Backing Up the Junos Space Network Management Platform Database to a Local Directory on page 687](#)
- [Backing Up the Junos Space Network Management Platform Database to a Remote Host on page 690](#)

Backing Up the Junos Space Network Management Platform Database to a Local Directory

To back up the Junos Space Network Management Platform database to a local directory:

1. On the Junos Space Network Management Platform user interface, select **Administration > Database Backup and Restore**.

The Database Backup and Restore page appears.

2. Click the **Database Backup** icon.

The Database Backup page appears. The default behavior is a backup operation that occurs once weekly (see the **Repeat** section on this page).

3. Retain the selection of **local** in the **Mode** field in the **Mode Options** section to back up the Junos Space Network Management Platform database to the default directory **/var/cache/jboss/backup**.



NOTE: When the local mode option is selected, the Username, Password, Confirm password, Machine IP, and Directory fields on the Database Backup page are disabled.

4. Retain the selection of **Network Monitoring** in 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.

5. (Optional) In the **Comment** field, add a comment to describe or otherwise identify the backup operation.
6. (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 operation.
 - Clear the **Schedule at a later time** check box (the default) to initiate the database backup operation as soon as you click **Backup**.



NOTE: The selected time in the scheduler corresponds to the Junos Space server time but uses the local time zone of the client computer.

7. (Optional) Schedule database backup recurrence by selecting **Repeat**. The default behavior is a backup operation that occurs once weekly.
 - a. Specify the database backup recurrence by setting the interval and the increment. The default recurrence interval is 1 hour.

Table 87: Backup Schedule Units and Increments

Unit of Time	Increment
Minutes	1–59
Hourly	12:00 AM–11:45 PM
Daily	For the specified number of days
Weekly	For the specified number of weeks on the selected days
Monthly	<p>For the specified number of months. The day on which the backup is performed is displayed. Usually, it is the current day. For example, if you are configuring this setting on Jul 10, 2013, the following are displayed:</p> <ul style="list-style-type: none"> • the 10th of the month.—This is the first option and is selected by default. If this option is selected, then the database is backed up every tenth of the month for the specified number of months. • the 2nd Wednesday of the month.—If this option is selected, then the database is backed up every second Wednesday of the month for the specified number of months.
Yearly	<p>For the specified number of years. The day on which the backup is performed is displayed. Usually, it is the current day. For example, if you are configuring this setting on Jul 10, 2013, the following are displayed:</p> <ul style="list-style-type: none"> • the 10th of July.—This is the first option and is selected by default. If this option is selected, then the database is backed up every tenth of July for the specified number of years. • the 2nd Wednesday of July.—If this option is selected, then the database is backed up every second Wednesday of July for the specified number of years.

- b. Specify when the recurrence should end in the **Ends on** section.

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.

8. Click **Backup**.

A confirmation dialog box appears, which displays:

Warning: Taking database backup may have an impact on system performance. Do you want to continue?

9. Click **OK** on the confirmation dialog box to back up the Junos Space database.

The **Backup Job Information** dialog box appears. Perform one of the following actions:

- Click the Job ID on this dialog box to view the database backup job details on the Job Management page.
- If you do not wish to view the job details (that is, whether the database backup job is a success or a failure), click **OK** on this dialog box. You are returned to the Database Backup and Restore page. If the backup job is successful, the new backup file is displayed on this page.

- Click **Cancel** on this dialog box to cancel the database backup operation.

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.

For troubleshooting, see the following logs on the Junos Space server:

- /var/log/nma.log
- /var/log/nma/*.log
- /tmp/maintenance.log

Backing Up the Junos Space Network Management Platform Database to a Remote Host

The protocol used to transfer the Junos Space Network Management Platform database backup to a remote host is Secure Copy Protocol (SCP).

To back up the Junos Space Network Management Platform database to a remote host:

1. On the Junos Space Network Management Platform user interface, select **Administration > Database Backup and Restore**.

The Database Backup and Restore page appears.

2. Click the **Database Backup** icon.

The Database Backup page appears. The default behavior is a backup operation that occurs once weekly (see the **Repeat** section on this page).

3. In the **Mode** field in the **Mode Options** section, select **remote**.
4. In the **Username** field, enter a username to access the remote host server.
5. In the **Password** field, enter the corresponding password.
6. In the **Confirm password** field, reenter the password.
7. In the **Machine IP** field, enter the remote host server IP address.
8. In the **Directory** field, enter a directory path on the remote host server where you want to store the database backup file.



NOTE: The directory path must already exist on the remote host server.

9. Retain the selection of **Network Monitoring** in 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.

10. (Optional) Add a comment to describe or otherwise identify the backup operation.

11. (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 operation.
- Clear the **Schedule at a later time** check box (the default) to initiate the database backup operation as soon as you click **Backup**.



NOTE: The selected time in the scheduler corresponds to the Junos Space server time but uses the local time zone of the client computer.

12. (Optional) Schedule database backup recurrence by selecting **Repeat**. The default behavior is a backup operation that occurs once weekly.

- a. Specify the database backup recurrence by setting the interval and the increment. See [Table 87 on page 689](#).

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 operation will recur endlessly until you cancel the job manually.

13. Click **Backup**.

A confirmation dialog box appears, which displays:

Warning: Taking database backup may have an impact on system performance. Do you want to continue?

14. Click **OK** on the confirmation dialog box to back up the Junos Space database.

The **Backup Job Information** dialog box appears. Perform one of the following actions:

- Click the Job ID on this dialog box to view the database backup job details on the Job Management page.
- If you do not wish to view the job details (that is, whether the database backup job is a success or a failure), click **OK** on this dialog box. You are returned to the Database

Backup and Restore page. If the backup job is successful, the new backup file is displayed on this page.

- Click **Cancel** on this dialog box to cancel the database backup operation.

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.

For any troubleshooting, see the following logs on the Junos Space server:

- `/var/log/nma.log`
- `/var/log/nma/*.log`
- `/tmp/maintenance.log`

Related Documentation

- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 692](#)
- [Viewing Database Backup Files on page 696](#)
- [Deleting Junos Space Network Management Platform Database Backup Files on page 698](#)
- [Backing Up and Restoring the Database Overview on page 684](#)
- [Viewing Audit Logs on page 604](#)
- [Viewing Scheduled Jobs on page 500](#)

Restoring the Junos Space Network Management Platform Database Through the Junos Space 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 shut down 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. After the restore database operation is completed, Junos Space Network Management Platform is restarted and users can access the Junos Space user interface.

Because you can back up the Junos Space database locally (that is, in the Junos Space server) or remotely (in another system), both the database backup files are displayed in the Junos Space GUI. You can restore the Junos Space database from the local or remote database backup file.

To restore a Junos Space Network Management Platform database, you must have System Administrator privileges and be a Maintenance Mode administrator.



NOTE: Before you restore a Junos Space Network Management Platform database, wait until all jobs that are currently running are completed.

To view information about the available database backup files before you select a Junos Space Network Management Platform database to restore, see [“Viewing Database Backup Files” on page 696](#).

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 Junos Space Network Management Platform Database Through the Junos Space User Interface on page 693](#)
- [Restoring the Junos Space Network Management Platform Database from a Remote File Through the Junos Space User Interface on page 694](#)

Restoring a Local Junos Space Network Management Platform Database Through the Junos Space User Interface

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.

In a multinode setup, the selected backup file may exist on both the primary and secondary nodes. The **Machine** column on the Database Backup and Restore page reflects the IP addresses of these nodes where the backup file is stored. In such cases where the same backup file exists on more than one node, Junos Space selects a backup file from one of the nodes randomly for the restore operation.

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?



CAUTION: This confirmation dialog box must display the name of the backup file that you selected for the restore operation. If not, wait for a few seconds until the backup filename appears before you proceed to the next step. Otherwise, the restore operation may fail.

4. Click **Continue** in the Restore confirmation 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 Junos Space Network Management Platform Database from a Remote File Through the Junos Space User Interface

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. On the Junos Space Network Management Platform user interface, select **Administration > Database Backup and Restore**.

The Database Backup and Restore page appears.

2. Click the **Restore From Remote File** icon.

The Restore From Remote File page appears.

3. In the **Username** field, enter a username to access the remote host server.
4. In the **Password** field, enter the corresponding password.
5. In the **Confirm password** field, reenter the password.
6. In the **Machine IP** field, enter the IP address of the device on which the backup file is located.
7. In the **File Path** field, enter the path to the backup file on that device.
8. (Optional) In the **Comment** field, enter a comment to capture any information about this database restore operation.
9. Click **Restore** to start the restore database operation.

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.

10. 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.

11. Enter the maintenance mode username and password.
12. 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.

13. In the Restore Database Status dialog box, click **Return to Maintenance Menu**.

The Maintenance Mode Actions dialog box appears.

14. 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 686](#)
 - [Viewing Database Backup Files on page 696](#)
 - [Deleting Junos Space Network Management Platform Database Backup Files on page 698](#)
 - [Maintenance Mode Overview on page 621](#)

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 operation, the backup file name and location, and the IP address of the Junos Space Appliance that is 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 696](#)
- [Viewing Database Details on page 696](#)
- [Managing Database Commands on page 697](#)

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. On the Junos Space Network Management Platform user interface, 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. On the Junos Space Network Management Platform user interface, select **Administration > Database Backup and Restore**.
The Database Backup and Restore page appears.
2. Double-click a database in tabular view. The View Backup page appears.
[Table 88 on page 697](#) defines the database backup detailed information.

Table 88: Fields in the Manage Databases Table

Field	Description
Name	Name of the database backup file. Junos Space Network Management Platform automatically assigns a name to the backup file.
Backup Date	Date and time of the database backup operation
Comment	Information a Junos Space user optionally provides in the Comments field of the Backup page when scheduling a database backup operation
Machine	IP address of the Junos Space Appliance on which the database backup operation is performed. In a multinode setup, the backup operation is initiated on the secondary node. When the backup operation is successfully completed, the backup file is synchronized with (copied to) the primary node. In such scenarios, the backup file exists on both the primary and secondary nodes, and the IP addresses of both the nodes are displayed in the Machine field.
File Path	File path for the database backup. For a local backup operation, this column displays the default directory location where the backup file is stored, which is: /var/cache/jboss/backup . For a remote backup operation, this column displays the path to the backup file on the remote server.

Managing 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 698](#)
- Restore Database—[“Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface” on page 692](#)
- Tag It—[“Tagging an Object” on page 793](#)
- View Tags—[“Tagging an Object” on page 793](#)
- Clear All Selections—Clears all selections you made on the Database Backup and Restore page.

Related Documentation

- [Deleting Junos Space Network Management Platform Database Backup Files on page 698](#)
- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 692](#)
- [Backing Up the Junos Space Network Management Platform Database on page 686](#)
- [Tagging an Object on page 793](#)

Deleting Junos Space Network Management Platform 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.
- In a multinode setup, the selected backup file may exist on both the primary and secondary nodes. The Machine column on the Database Backup and Restore page reflects the IP addresses of these nodes where the backup file is stored. In such cases where the same backup file exists on more than one node, when you delete a backup file, the backup file is deleted from both the nodes.

To delete a Junos Space Network Management Platform database backup file:

1. On the Junos Space Network Management Platform user interface, select **Administration > Database Backup and Restore**.

The Database Backup and Restore page appears.

2. From the Database Backup and Restore page tabular 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 the **Delete Backup** icon on the toolbar.

Junos Space Network Management Platform deletes the selected Junos Space Network Management Platform database backup files. The deleted backup files are no longer displayed on the inventory page and are deleted from the `/var/cache/jboss/backup` directory if it is a local backup operation or from the remote location for a remote backup operation.



CAUTION: When you delete a local backup file, if the backup file is present on both the primary and secondary nodes, then this file is deleted from both the nodes.

When you delete a database backup file, an audit log entry is automatically generated and details about the deleted file is recorded.

To obtain details about the backup files that were deleted from an audit log entry:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs > Audit Log**.

The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using the **Delete Backup** keyword.

The Audit Log page displays only the audit log entries that were generated when the database backup files were deleted.

3. Double-click an audit log entry.

The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of database backup files that were deleted and the **Affected Object Detail** section displays details about each database backup file.

4. Click **OK** on the Audit Log Detail page to exit this page.

You are returned to the Audit Log page.

Related Documentation

- [Backing Up the Junos Space Network Management Platform Database on page 686](#)
- [Restoring the Junos Space Network Management Platform Database Through the Junos Space User Interface on page 692](#)
- [Viewing Database Backup Files on page 696](#)

Viewing Database Backup 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. On the Junos Space Network Management Platform user interface, 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 686](#)
- [Viewing Scheduled Jobs on page 500](#)
- [Viewing Audit Logs on page 604](#)

Manage Licenses

- [Generating and Uploading the Junos Space License Key File on page 701](#)
- [Viewing Licenses on page 703](#)

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 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 Junos Space License Key File on page 702](#)
2. [Uploading the Junos Space License Key File Contents on page 702](#)

Generating the Junos Space 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 Junos Space License Key File Contents

To upload the Junos Space license key file, perform the following steps:

1. Open the Juniper Networks Authorization Codes e-mail you received and follow the directions.
2. Open the Junos Space 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 Junos Space license key text file in the **License data** field.

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 703](#)

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 701.

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 703](#)

Viewing License Details

Table 89 on page 703 defines the license details.

Table 89: Licenses Details

Field	Description
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.

Table 89: Licenses Details (*continued*)

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

- [Exporting License Inventory on page 47](#)

CHAPTER 69

Manage Applications

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Modifying Network Management Platform Settings on page 711](#)
- [Configuring Password Rules for Junos Space Network Management Platform on page 714](#)
- [Managing Services on page 718](#)
- [Configuring Network Activate Application Settings on page 721](#)
- [Adding a Junos Space Application on page 721](#)
- [Junos Space Software Upgrade Overview on page 724](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Upgrading Junos Space Software Overview on page 727](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Uninstalling a Junos Space Application on page 733](#)

Managing Applications Overview

You can use the Applications workspace to manage Junos Space Network Management Platform and all other separately packaged applications.

In this workspace, you can perform the following tasks:

- Install a new Junos Space application by using the **Administration > Applications > Add Application** task (see [“Adding a Junos Space Application” on page 721](#)).
- Upgrade Junos Space Network Management Platform by using the **Administration > Applications > Upgrade Platform** action (see [“Upgrading Junos Space Network Management Platform” on page 729](#)). Junos Space Network Management Platform provides the running environment for all Junos Space applications, so upgrading it interrupts the operation.
- Upgrade a Junos Space application while Junos Space Network Management Platform is still running by using the **Administration > Applications > Upgrade Application** action (see [“Upgrading a Junos Space Application” on page 725](#)).

- Uninstall a Junos Space application while Junos Space Network Management Platform is still running by using the **Administration > Applications > Uninstall Application** action (see “[Uninstalling a Junos Space Application](#)” on page 733).
- Modify application settings by using the **Network Management Platform > Administration > Applications > Modify Application Settings** action (see “[Modifying Junos Space Application Settings](#)” on page 709).
- Start, stop, or restart services by using the **Administration > Applications > Manage Services** action (see “[Managing Services](#)” on page 718).
- Tag applications to categorize them for filtering and performing Manage Applications actions by using the **Administration > Applications > Tag It** action (see “[Tagging an Object](#)” on page 793).
- View tags that you have already created on a selected application by using the **Network Management Platform > Administration > Applications > View Tags** action (see “[Viewing Tags for a Managed Object](#)” on page 794).



NOTE: The Junos Space Network Management Platform Upgrade image includes 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 support site (<https://www.juniper.net/support/products/space/#sw>) to the local client file system. The administrator must upload an application file to the Junos Space Network Management Platform. After the application file is 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 the workspace of an upgraded application are directed to Application Chooser.

Related Documentation

- [Managing Junos Space Applications on page 706](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Uninstalling a Junos Space Application on page 733](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)

Managing Junos Space Applications

Manage Junos Space applications from the **Administration > Applications** task. All applications that you have uploaded and installed appear on the **Applications** inventory

page. You need Super Administrator or System Administrator privileges. From the Applications inventory page, you can manage Junos Space hot-pluggable applications, such as installation, upgrading, and uninstallation, 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 will interrupt normal operations of Junos Space Network Management Platform. 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 simultaneously.

- [Installing or Upgrading a Junos Space Application on page 707](#)
- [Viewing Detailed Information About the Junos Space Application on page 707](#)
- [Performing Actions on the Junos Space Applications on page 708](#)

Installing or Upgrading a Junos Space Application

To install or upgrade a Junos Space application:

1. Download a new Junos Space application from the Juniper Networks software download site to the local client machine.
2. To add the application, upload the application to Junos Space Network Management Platform by selecting **Administration > Applications** and clicking the Add Application icon. To upgrade the 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 Applications inventory page. The new or upgraded application appears in Application Chooser (at the upper-left corner).

Viewing Detailed Information About the Junos Space Application

[Table 90 on page 707](#) describes the information displayed in table columns for each application on the Applications inventory page.

Table 90: Application Information

Application Information	Description
Title	Name of the Junos Space application
Version	Version of the Junos Space application software
Release Type	Release type of the Junos Space application software
Build	Build number of the Junos Space application software

Table 90: Application Information (*continued*)

Application Information	Description
Server Group	<p>Server group to which the application belongs. For more information on server group, see “Running Applications in Separate Server Instances” on page 622.</p> <p>By default, all applications belong to the platform server group unless you added an application to another server group. For more information about adding an application to a server group, see “Adding a Junos Space Application” on page 721.</p>

Performing Actions on the Junos Space Applications

You can perform the following actions on the Junos Space applications from the 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 709](#).



NOTE: This action is available for Junos Space Network Management Platform only.

- **Refresh Search Index**—Click to refresh the search index to keep it current with the changes made to the database. By default, the search index is refreshed every five seconds. You can modify this duration from **Administration > Applications > Network Management Platform > Modify Application Settings > Search > Index auto update interval in seconds**. You are prompted to confirm that you want to refresh the search index. Click **OK** to confirm.
- **Manage Services**—See [“Managing Services” on page 718](#).
- **Upgrade Platform**—See [“Upgrading Junos Space Network Management Platform” on page 729](#).



NOTE: This action is available for Junos Space Network Management Platform only.

- **Upgrade Application**—See [“Upgrading a Junos Space Application” on page 725](#).
- **Uninstall Application**—See [“Uninstalling a Junos Space Application” on page 733](#).
- **Delete Private Tags**—Delete private tags; that is, delete tags that you created.
- **Tag It**—See [“Tagging an Object” on page 793](#).
- **Untag It**—[“Untagging Objects” on page 794](#).
- **View Tags**—See [“Viewing Tags for a Managed Object” on page 794](#).

Related Documentation

- [Managing Applications Overview on page 705](#)
- [Adding a Junos Space Application on page 721](#)

- [Upgrading Junos Space Software Overview on page 727](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Uninstalling a Junos Space Application on page 733](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)
- [Untagging Objects on page 794](#)

Modifying Junos Space Application Settings

As the Super Administrator or system administrator, you can modify Junos Space application settings.

To modify Junos Space application settings:

1. Select **Administration > Applications**.

The **Applications** inventory page appears.

2. Select the application for which you want to modify the settings.

For example, 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 that you are managing:

- [Modifying Network Management Platform Settings on page 711](#)
- [Configuring Network Activate Application Settings on page 721](#)

5. Click **Modify**.



NOTE: You cannot modify the application settings if another user is currently modifying the application settings. You 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**

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)
- [Uninstalling a Junos Space Application on page 733](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Creating a Tag on page 798](#)
- [Managing Tags on page 781](#)

Modifying Network Management Platform Settings

Table 91 on page 711 lists the application settings that you can configure for Junos Space Network Management Platform. You must have Super Administrator or System Administrator privileges.

Table 91: 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. By default, this check box is selected.
	Enable approval workflow for configuration deployment	This option is for candidate configuration (previously known as consolidated configuration). This option lets a user deploy any configuration changes made from Junos Space Network Management Platform on to a device only on approval. By default, this check box is selected. By clearing this check box, you can deploy the configuration directly without approval.
	Junos Space 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.

Table 91: Junos Space Network Management Platform Application Settings (*continued*)

Category	Parameter Label	Description
	Number of devices to connect per minute for Space Initiated Connection	This parameter enables you to throttle the number of devices that connect to Junos Space Network Management Platform. 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 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	This 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. By default, this check box is unselected.
	Space as system of record choices	<p>This setting specifies the system of record: network (NSOR, which is the default) or Junos Space Network Management Platform (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 825.</p>

Table 91: Junos Space Network Management Platform Application Settings (*continued*)

Category	Parameter Label	Description
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 login only. <p>For more information, see “Limiting User Sessions” in “Creating User Accounts” on page 571.</p>
	UI auto refresh interval in seconds	<p>This text box specifies the time, in seconds, after which the Junos Space GUI is refreshed automatically. The default value is three seconds. You can enter a value from 1 through 92,23,37,20,36,85,47,76,000.</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 Rules for Junos Space Network Management Platform” on page 714 .	
Audit Log	Record HTTP GET method	<p>This check box audit logs all API GET calls. By default, this check box is unselected.</p>

Table 91: 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%.
Configs	Advanced Xpath Processing	<p>If this check box is selected, whenever you trigger an action on a device that requires BaseX support, the BaseX database is populated for that device across the Junos Space nodes. Any resynchronization or discovery triggered after the configuration is enabled, is handled.</p> <p>If this check box is unselected (the default), then BaseX database is not used.</p>
Related Documentation	<ul style="list-style-type: none"> • Modifying Junos Space Application Settings on page 709 • Configuring Password Rules for Junos Space Network Management Platform on page 714 • Worldwide Junos OS Adapter Overview on page 145 • Systems of Record in Junos Space Overview on page 825 	

Configuring Password Rules for Junos Space Network Management Platform

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 Junos Space Network Management Platform Release 12.1 or later, these default password settings take effect immediately. All local users receive password expiration messages the first time they log in after the upgrade.

You click the User Preferences (see [“Changing Your Password on Junos Space” on page 5](#)) to create a new password, but the constraints that govern this password are set in the Administration workspace. This topic describes the parameters that limit password creation and how to set them.

All users creating their passwords can view the parameters set by the Junos Space administrator. To display the rules, 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 92 on page 715](#) describes all the parameters for password rules.

Table 92: 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 numerals, 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 the 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 log in 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>

Table 92: Password Constraint Parameters (*continued*)

Parameter	Default (yes, no, or default value)	Explanation or Example
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 log in because they have entered incorrect 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 third attempt.</p> <p>NOTE: You can unlock a locked-out user at any time (see “Disabling and Enabling Users” on page 581).</p>
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 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” field). 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.

Table 92: Password Constraint Parameters (*continued*)

Parameter	Default (yes, no, or default value)	Explanation or Example
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 .
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 92 on page 715](#) for guidance.

5. Click **Modify** to apply your choices.

For troubleshooting, see the `/var/log/jboss/servers/server1/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 581](#)
- [Creating User Accounts on page 571](#)
- [Managing Applications Overview on page 705](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Modifying Junos Space Application Settings on page 709](#)

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 93: 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 synchronization 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.
	E-mail 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	The service continues to be operational even if Junos Space Network Management Platform is rebooted.
	An 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. 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 on 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 that can be 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 Service**, **Restart Service**, or **Stop Service**.

One of four messages appears:

- If you select a service that is currently running, then select **Stop Service**, 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 Service**, 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 Service**, 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 Service**, 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 click only **OK**.

You first receive a message indicating that the relevant action is being performed. This is followed by a second status message indicating whether the operation you performed was successful or not.

5. Click **OK** to confirm.

The Manage Services page reappears, displaying the changed status of the selected service.

**Related
Documentation**

- [Managing Applications Overview on page 705](#)
- [Junos Space Audit Logs Overview on page 603](#)
- [Role-Based Access Control Overview on page 519](#)

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 709](#).

You must have Super Administrator privileges to configure Network Activate application settings.

[Table 94 on page 721](#) defines the application settings you can configure for the Network Activate application settings.

Table 94: Network Activate Application Settings

Category	Application Setting Name	Description
Deployment	Deploy configuration to the device	Disable this setting to deploy the configuration to the 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 by using the Junos OS curly braces syntax.
	Use vlanmaps for flexible tagged services	Enable this setting if the 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 709](#)

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 725](#).

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 Networks software download site to the local client file system:

<https://www.juniper.net/support/products/space/#sw>

2. Select **Administration > Applications** and click 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 steps:

- 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 13.3R1, 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. In the **Username** field, enter your username.
- ii. In the **Password** field, enter your password.
- iii. In the **Confirm password** field, enter your password again to confirm the password.
- iv. In the **Machine IP** field, enter the host IP address.
- v. In the **Software File Path** field, enter the path name of the Junos Space 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 13.3R1, 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** and click the **Add Application** icon.

The Add Application page appears.

2. Select the uploaded application.
3. Click **Install** to install the application or click **Cancel** to exit the Add Application page.

The Application configuration page appears, displaying a list of server groups to which you can deploy the application.



CAUTION: After you select and successfully deploy an application to a server group, it is not possible to move the application from one server group to another from the Junos Space GUI. So choose a server group after careful consideration. To move an application from one server group to another, use the script tool (see the instructions specified in [“Running Applications in Separate Server Instances” on page 622](#)).

4. Select a server group to which you want to deploy the application.

The default server group is **platform** to which Junos Space Network Management Platform is deployed. If you do not select any server group, the selected application is automatically deployed to the default **platform** server group.

5. Click **OK** to proceed.

The Application Management Job Information dialog box appears.

6. 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 of the application is a failure, then the Summary column for the installation job displays the reason for 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.** However, the display of such messages depends also 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.

7. 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

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Uninstalling a Junos Space Application on page 733](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)

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 on the Junos Space Network Management Platform 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 Virtual Appliances, complete the following tasks before performing the upgrade:

- 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: <https://www.juniper.net/support/products/space/#sw>



CAUTION: We recommend that you do not change the name of the software image that you download from the Juniper support site before you upload it to Junos Space Network Management Platform.

- 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 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, click the Help icon on the user interface banner and click **About**.

Related Documentation

- [Upgrading Junos Space Software Overview on page 727](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)

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. After the application is upgraded successfully, you can launch it from Application Chooser.

To upgrade an existing Junos Space application:

1. Download the application to which you want to upgrade from the Juniper Software download site to the local client file system.

<https://www.juniper.net/support/products/space/#sw>



CAUTION: It is recommended not to change the name of the software image that you downloaded from the Juniper support site before you upload it to Junos Space Network Management Platform.

2. Select **Administration > Applications**. The Applications inventory page appears.
3. Select the application that you want to upgrade.
4. Select **Upgrade Application** from the Actions menu.

The Upgrade Application dialog box appears displaying all previously uploaded versions of that application.

5. 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.

6. Navigate to the Application Chooser and launch the application you upgraded.



NOTE: To install a new Junos Space application, use the **Administration > Applications > Add Application** action, see [“Adding a Junos Space Application” on page 721](#).

Related Documentation

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)
- [Adding a Junos Space Application on page 721](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Uninstalling a Junos Space Application on page 733](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)

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 13.3R1 supports upgrading from 13.1, specifically from 13.1R1, 13.1P1.14, 13.1P5.3, and 13.1P6.3 release versions.

- [Junos Space 13.3R1 Release Highlights on page 727](#)
- [Before You Begin on page 728](#)
- [Upgrading Junos Space Release to Release 13.3R1 and Later Versions on page 728](#)

Junos Space 13.3R1 Release Highlights

The Junos Space Network Management Platform Upgrade Release 13.3R1 includes:

Junos Space Network Management Platform Release 13.3R1 Contents

- Network Management Platform Release 13.3R1—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 13.3R1
- Service Insight Release 13.3R1

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 13.3R1 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 [“Managing Applications Overview” on page 705](#).
 - 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 13.3R1 and Later Versions

The Platform provides the running environment for all Junos Space applications. Hence, the operations of the applications are interrupted during the upgrade.



NOTE: When upgrading Junos Space Network Management Platform to 13.3R1 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 13.3R1 are enabled. Other applications running on Junos Space Network Management Platform with releases prior to 13.3R1 and that are not supported with Junos Space Network Management Platform Release 13.3R1 might be disabled. You must upgrade these disabled applications to release 13.3R1. (see [“Upgrading a Junos Space Application” on page 725](#)) or uninstall them (see [“Uninstalling a Junos Space Application” on page 733](#)). Do not add disabled Junos Space applications using Platform > Administration > Applications > Add Application.

To upgrade Junos Space Network Management Platform from release 13.1 to release 13.3R1, see [“Upgrading Junos Space Network Management Platform” on page 729](#).

Related Documentation

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)

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 13.3R1 supports upgrading from 13.1, specifically from 13.1R1, 13.1P1.14, 13.1P5.3, and 13.1P6.3 release versions.



NOTE: When you perform an upgrade to Junos Space Network Management Platform release 13.3R1 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.



CAUTION: You should not change the name of the software image that you downloaded from the Juniper support site before you upload it to Junos Space Network Management Platform. The software installation fails if you make even a slight modification to the filename.

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**.



CAUTION: However, if the following error message appears, it is recommended that you try uploading the image by using the **Upload via SCP** option.

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

- 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. Confirm 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 13.3R1, 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 686](#) 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 **Reboot Junos Space** 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.



NOTE: When you upgrade Junos Space Network Management Platform to version 13.3R1 on a multi-node setup and initiate a reboot request, the nodes are rebooted as follows:

1. The master node starts the reboot process. The other nodes stay in the DOWN state (i.e. jboss, jmp-watchdog, heartbeat services are in the Stopped state).
2. The master node completes the reboot, deploys the .ear files, and finishes the initialization process.
3. The master node issues a reboot request to all other nodes when it is in the process of deploying the appmgt .ear file.
4. The other nodes reboot and start the process of deploying the .ear files and initialization.
5. The total time for all the nodes to completely initialize would be longer than that for the previous releases.

Though you can access the Junos Space GUI after the VIP node is up, it is recommended that you wait until all the nodes in the fabric are up. To determine whether rest of the nodes are up, verify the status of each node on the **Administration > Fabric inventory** landing page.

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/servers/server1/server.log**—This file captures information about JBoss.

Related Documentation

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Uninstalling a Junos Space Application on page 733](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)

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. Association between the uninstalled application and the server group from which it has been uninstalled is lost. The server group itself is not removed by the uninstallation of an application. However, if you

want to delete the server group along with the application, use the JBoss Management CLI (see [“Running Applications in Separate Server Instances” on page 622](#)).

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

The display of such messages depends 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**

- [Managing Applications Overview on page 705](#)
- [Managing Junos Space Applications on page 706](#)
- [Running Applications in Separate Server Instances on page 622](#)
- [Modifying Junos Space Application Settings on page 709](#)
- [Upgrading a Junos Space Application on page 725](#)
- [Upgrading Junos Space Network Management Platform on page 729](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)

CHAPTER 70

Troubleshoot Space

- [System Status Log File Overview on page 735](#)
- [Customizing Node System Status Log Checking on page 737](#)
- [Customizing Node Log Files To Download on page 738](#)
- [Downloading the Troubleshooting Log File in the Server Mode on page 738](#)
- [Downloading the Troubleshooting Log File in the Maintenance Mode on page 740](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 740](#)

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 735](#).

The system administrator can customize the information that is collected in the system log file. See [“Customizing Node System Status Log Checking” on page 737](#).

The system administrator can download the latest log files for each fabric node when logged in to a Junos Space Appliance. See [“Downloading System Log Files for a Junos Space Appliance” on page 736](#).

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 738](#).

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 737](#).

Downloading System Log Files for a Junos Space Appliance

The system administrator can download the latest log files for each fabric node when logged in to 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 95 on page 736](#) lists the files included in the **troubleshoot** file.

Table 95: Log Files included in the troubleshoot File

Description	Location
System status log files	<code>/var/log/SystemStatusLog</code>
JBoss log files	<code>/var/log/jboss/*</code>
Service-provisioning data files	<code>/var/tmp/jboss/debug/*</code>
MySQL error log files	<code>/var/log/mysqld.log</code>
Log files for Apache, Node Management Agent (NMA), and Webproxy	<code>/var/log/httpd/*</code>
Watchdog log files	<code>/var/log/watchdog/*</code>
System messages	<code>/var/log/messages/*</code>

The system administrator can download log files in each operation mode as follows:

- Server mode (See [“Downloading the Troubleshooting Log File in the Server Mode” on page 738](#).)
- Maintenance mode (See [“Downloading the Troubleshooting Log File in the Maintenance Mode” on page 740](#).)
- CLI mode (See [“Downloading Troubleshooting System Log Files Through the CLI” on page 740](#).)

Customizing Log Files to Download

The system administrator can also customize the log files to be downloaded for specific fabric nodes. For more information about customizing node log files to download, see [“Customizing Node Log Files To Download” on page 738](#).

Related Documentation

- [Customizing Node System Status Log Checking on page 737](#)
- [Customizing Node Log Files To Download on page 738](#)

- [Downloading the Troubleshooting Log File in the Server Mode on page 738](#)
- [Downloading the Troubleshooting Log File in the Maintenance Mode on page 740](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 740](#)

Customizing Node System Status Log Checking

You customize the system status checking for a fabric node to ensure that all necessary information is written to the `/var/log/SystemStatusLog` log file. You must have the privileges of a System Administrator to customize the system status checking. You customize the system status checking by modifying the fabric node Perl script in `/usr/nma/bin/writeLogCronJob`.

To customize system status checking for a fabric node, 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

- [System Status Log File Overview on page 735](#)
- [Customizing Node Log Files To Download on page 738](#)
- [Downloading the Troubleshooting Log File in the Server Mode on page 738](#)
- [Downloading the Troubleshooting Log File in the Maintenance Mode on page 740](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 740](#)

Customizing Node Log Files To Download

You customize the log files downloaded for a fabric node to ensure that you download all the necessary log files. You must have the privileges of a System Administrator to customize the log files. You customize the log files you want to download by modifying the Perl script in `/var/www/cgi-bin/getLogFiles`.

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

- [System Status Log File Overview on page 735](#)
- [Customizing Node System Status Log Checking on page 737](#)
- [Downloading the Troubleshooting Log File in the Server Mode on page 738](#)
- [Downloading the Troubleshooting Log File in the Maintenance Mode on page 740](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 740](#)

Downloading the Troubleshooting Log File in the Server Mode

You download the troubleshooting log file in the Server mode when you want to view the contents of the troubleshooting log file and fix issues. You need to have the privileges of a System Administrator to download the troubleshooting log file.

To download the troubleshooting log file in the Server mode:

1. On the Junos Space Network Management Platform user interface, select **Administration > Space Troubleshooting**.
The Space Troubleshooting page is displayed.
2. Click the **Download** 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 page, 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_yyyy-mm-dd_hh-mm-ss.zip` file.

Table 96 on page 739 lists the files included in the `troubleshoot_yyyy-mm-dd_hh-mm-ss.zip` file.

Table 96: Data and Log Files in troubleshooting log 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

- [System Status Log File Overview on page 735](#)
- [Customizing Node System Status Log Checking on page 737](#)
- [Customizing Node Log Files To Download on page 738](#)
- [Downloading the Troubleshooting Log File in the Maintenance Mode on page 740](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 740](#)

Downloading the Troubleshooting Log File in the 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 shut down 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, perform the following 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.

2. Click the **click here to log in** link. The login dialog box appears.
3. Log in to maintenance mode by 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 621](#)
- [System Status Log File Overview on page 735](#)
- [Customizing Node System Status Log Checking on page 737](#)
- [Customizing Node Log Files To Download on page 738](#)
- [Downloading the Troubleshooting Log File in the Server Mode on page 738](#)
- [Downloading Troubleshooting System Log Files Through the CLI on page 740](#)

Downloading Troubleshooting System Log Files Through the CLI

If Junos Space Network Management Platform is running, the administrator can log in to a Junos Space Appliance console and download system status logs for each fabric node by using the CLI Network Settings Utility > SecureCoPy (SCP) command. If the system is not operating, the administrator can download system status logs using the by 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 about the log files that are written, see [“System Status Log File Overview” on page 735](#).

This procedure includes the following tasks:

- [Downloading a System Log File by Using a USB Device on page 741](#)
- [Downloading System Log File by Using SCP on page 742](#)

Downloading a System Log File by 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. Typically, use the default administrator credentials to log in to the Junos Space Appliance (admin/abc123).

Junos Space Settings Menu

```
1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> (Debug) run shell
```

```
Q> Quit
R> Redraw Menu
```

Choice [1-6,QR]:

2. Type option 4. The Retrieve Logs submenu appears.

```
Choice [1-6,AQR]: 4
1> Save to USB Device
2> Send Using SCP
```

```
A> Apply changes
M> Return to Main Menu
R> Redraw Menu
```

Choice [1-2,AMR]:

3. Select 1. The USB device must be connected to a Junos Space Appliance.

The following message appears:

This process will retrieve the log files on all cluster members and combine them into a .tar file. Once the file is created, you can copy the files onto a USB drive. Continue? [y/n]

4. Indicate whether you want to continue. Enter **y** for yes; **n** to abort.
5. Enter the local administrator password (typically, the password is “abc123”).
6. The Save to USB process downloads the log files from all cluster members and combines them into a **.tar** file. After the file is created, the process copies the file to a USB device. You see the following message:

Copying 20090827-1511-logs.tar to USB drive

If the USB device is not ready, the following message appears:

Log collection complete If USB key is ready, press "Y". To abort, press "N".

Downloading System Log File by 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 by using SCP, perform the following 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> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> (Debug) run shell
```

```
Q> Quit
R> Redraw Menu
```

Choice [1-6,QR]:

2. Type option 4. The Retrieve Logs submenu appears.

```
Choice [1-6,AQR]: 4
1> Save to USB Device
2> Send Using SCP
```

```
A> Apply changes
M> Return to Main Menu
R> Redraw Menu
```

Choice [1-2,AMR]:

3. Select 2. The process retrieves the log files on all cluster members and combines them into a .TAR file as you can see from the following message:

This process will retrieve the log files on all cluster members and combine them into a .tar file. Once the file is created, you will be asked for a remote scp server to transfer the file to. Continue? [y/n]

4. Indicate whether you want to continue. Enter **y** for yes; **n** to abort.
5. Enter the local administrator password (typically, the password is "abc123").
6. Specify the SCP server IP address to which to transfer the file.
7. Enter the remote SCP user. For example, **root**
8. Enter the remote SCP file location. For example, **/root/tmplogs**. You see the following output:

```

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

```

9. Indicate whether the SCP server information is correct. Enter **y** for yes; **n** if incorrect.
10. Indicate whether you want to continue. Enter **y** for yes; **n** for no.

Related Documentation

- [Maintenance Mode Overview on page 621](#)
- [System Status Log File Overview on page 735](#)
- [Customizing Node System Status Log Checking on page 737](#)
- [Customizing Node Log Files To Download on page 738](#)
- [Downloading the Troubleshooting Log File in the Server Mode on page 738](#)
- [Downloading the Troubleshooting Log File in the Maintenance Mode on page 740](#)

CHAPTER 71

Manage Certificates

- [Certificate Management Overview on page 745](#)
- [Installing Custom SSL Certificate on the Junos Space Server on page 751](#)

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 Secure Sockets Layer (SSL) connection is the most secure type of authentication. The certificates can be stored on a smart card, a universal serial bus (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 745](#)
- [Loading a Custom Junos Space Server Certificate on page 747](#)
- [Loading a User Certificate on page 747](#)
- [Loading CA Certificates and CRLs on page 748](#)
- [Changing the Authentication Mode on page 749](#)
- [Invalid Certificates on page 750](#)

Workflow

The basic steps in establishing an SSL connection for the different modes of authentication are as follows:

- Certificate-based authentication:
 1. A client requests access to the Junos Space server.
 2. The Junos Space server presents its certificate to the client.
 3. The client verifies the server's certificate.
 4. If the verification of the certificate is successful, then the client sends its certificate to the server.

5. The server verifies the credentials of the client.
6. 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:
 1. A client requests access to the Junos Space server.
 2. The Junos Space server presents its certificate to the client.
 3. The client verifies the server's certificate.
 4. If the verification of the certificate is successful, then the client sends its username and password to the server.
 5. The server verifies the credentials of the client.
 6. 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 the Junos Space Network Management Platform.

In Junos Space Network Management Platform Release 13.1 and later both certificate-based authentication as well password-based authentication are supported. 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 certification authority (CA) certificates and the personal or user certificates (the Junos Space server certificate is optional) to the Junos Space server. Junos Space Network Management Platform verifies all certificates before 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 747](#).

2. Load the user certificate:

- For a new local user (from User > User Accounts > Create User inventory landing page).

See [“Loading a User Certificate” on page 747](#).

- For existing local users (from User > User Accounts > Modify User or User Preferences inventory landing page).

See [“Loading a User Certificate” on page 747](#).

3. Load the CA certificates and the certificate revocation list (from Administration > CA/CRL Certificates).

See [“Loading CA Certificates and CRLs” on page 748](#).

4. Enable certificate-based authentication mode (from Administration > Applications > Network Management Platform > Modify Application Settings > User > Use X509 Certificate Auth Mode option).

See [“Changing the Authentication Mode” on page 749](#).

Loading a Custom Junos Space Server Certificate

By default, Junos Space Network Management Platform uses a self-signed SSL certificate. 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 751](#).

Loading a User Certificate

If you opt to use 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). You can navigate to the Modify User page through **Role Based Access Control > User Accounts > Select a user > Modify 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 **Role Based Access Control > User Accounts > Create User** (icon). 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 the Create User page, see ["Creating User Accounts" on page 571](#).
 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 who is currently logged in:
 1. Click the **User Preferences** icon located at the top right-hand corner of the Junos Space Network Management Platform GUI (next to the Log Out icon). The Change Local Password and Certificate dialog box appears.
 2. Click the **X.509 Certificate** tab.
 3. In the **Certificate Subject Name** field, enter the string that needs to be secured. For example, it could be a person's e-mail, a Website address, or a system's IP address, and so on.
 4. Click **Browse** adjacent to the **X.509 Certificate File** field to navigate to the location of the X.509 certificate file on your local system.
 5. Click **Upload**.
 6. Click **OK**.
- To modify an existing user other than the user who is currently logged in:
1. Select **Role Based Access Control > User Accounts > Select a user > Modify User** (icon). 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 certification authority (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 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 down arrow next to the **+** icon and select **X.509 CA Certificate**.

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 down arrow 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 located at the top left-hand corner of the CA/CRL Certificates page. 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**.
2. From the Actions menu, select **Modify Application Settings**.

The Modify Network Management Platform Settings page appears.

3. Click **User**.

4. Select **Use X509 Certificate Auth Mode**.
5. Click **Modify**.



CAUTION: When the authentication mode is changed, all the existing user sessions are automatically terminated and all users, except the current administrator who is changing the authentication mode, are forced to log out.

If the certificate is scheduled to expire within 30 days from the current date, a warning message appears when the user logs in to indicate that the certificate will expire after these many days. Reload your certificate from the Change Local Password and Certificate page (by clicking the **User Preferences** icon at the top right-hand corner of the GUI) or request the administrator to reload it from the Modify User page (by clicking the **Modify User** icon from Role Based Access Control > User Accounts > Select a user). 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 from this directory location:
`./setSpaceAuthMode password-based`

This command sets the authentication mode to password-based for all users. When the authentication mode is changed, all the existing user sessions are automatically terminated and all users, except for the current administrator who is changing the authentication mode, are forced to log out.

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 the Junos Space server.

**Related
Documentation**

- [Installing Custom SSL Certificate on the Junos Space Server on page 751](#)

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 751](#)
- [Installing an X.509 Junos Space Server Certificate on page 751](#)
- [Installing a PKCS #12 Format Junos Space Server Certificate on page 752](#)
- [Certificate Expiry on page 753](#)
- [Certificate Attributes on page 753](#)

Changing the Default Junos Space Server SSL Certificate

By default, Junos Space Network Management Platform uses a self-signed SSL certificate. 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 97 on page 754](#).

2. To install an X.509 certificate, see [“Installing an X.509 Junos Space Server Certificate” on page 751](#).

To install a PKCS #12 format certificate, see [“Installing a PKCS #12 Format Junos Space Server Certificate” on page 752](#).

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 97 on page 754 lists the attributes that you commonly see in a certificate.

Table 97: Certificate Attributes

Certificate Attribute	Description
Subject Name: OID.1.2.840.113549.1.9.1=user1@10.205.57.195	<p>"OID.1.2.840.113549.1.9.1" is the ASN.1 object identifier used to identify this signature algorithm. "user1@10.205.57.195" is the e-mail address of the certificate owner.</p>
Subject Name: CN	Common name of the certificate owner
Subject Name: OU	<p>Name of the organizational unit to which the certificate owner belongs.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "Junos Space" for this attribute.</p>
Subject Name: O	<p>Organization to which the certificate owner belongs.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "Juniper Networks, Inc." for this attribute.</p>
Subject Name: L	<p>Certificate owner's location.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "Sunnyvale" for this attribute.</p>
Subject Name: ST	<p>Certificate owner's state of residence.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "California" for this attribute.</p>
Subject Name: C	<p>Certificate owner's country of residence.</p> <p>For example, "US."</p>
Issuer Name: OID.1.2.840.113549.1.9.1=user1@10.205.57.195	<p>"OID.1.2.840.113549.1.9.1" is the ASN.1 object identifier used to identify this signature algorithm. "user1@10.205.57.195" is the e-mail address of issuer.</p>
Issuer Name: CN	<p>Common name of the certificate issuer.</p> <p>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.</p>
Issuer Name: OU	<p>Name of the organizational unit to which the certificate issuer belongs</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "Junos Space" for this attribute.</p>
Issuer Name: O	<p>Organization to which the certificate issuer belongs.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "Juniper Networks, Inc." for this attribute.</p>
Issuer Name: L	<p>Certificate issuer's location.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "Sunnyvale" for this attribute.</p>

Table 97: Certificate Attributes (*continued*)

Certificate Attribute	Description
Issuer Name: ST	<p>Certificate issuer's state of residence.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "California" for this attribute.</p>
Issuer Name: C	<p>Certificate issuer's country of residence.</p> <p>For example, "US."</p>
Signature Algorithm Name	<p>Algorithm used by the Certificate Authority to sign the certificate.</p> <p>For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks can contain "SHA1withRSA" for this attribute.</p>
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 745](#)

CHAPTER 72

Manage Authentication Servers

- [Remote Authentication Overview on page 757](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Managing Remote Authentication Servers on page 759](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 764](#)
- [Configuring TACACS+ for Authentication and Authorization on page 768](#)
- [Junos Space Login Behavior with Remote Authentication Enabled on page 770](#)

Remote Authentication Overview

Junos Space Network Management Platform, by default, authenticates users to log in locally when you configure their accounts by using **Role Based Access Control > User Accounts > Create User** (icon) task.

On the **Administration > Authentication Servers** inventory landing page, you can authenticate users to log in exclusively from a centralized location by using one or more RADIUS or TACACS+ remote authentication servers. You can also authenticate users to log in to Junos Space Network Management Platform by 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 users by 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: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

You must have super administrator or 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 the users solely by a remote authentication server.

You may choose to allow some privileged users to set a local password so they can still log in to the Junos Space system if the remote authentication server is unreachable.

**Related
Documentation**

- [Junos Space Authentication Modes Overview on page 758](#)
- [Managing Remote Authentication Servers on page 759](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)
- [Junos Space Login Behavior with Remote Authentication Enabled on page 770](#)

Junos Space Authentication Modes Overview

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 **Role Based Access Control > User Accounts > Create User** (icon) task. You configure remote and remote-local authentication from **Administration > Authentication Servers > Use Remote Authentication > Remote Authentication Only/Remote-Local Authentication** task.



NOTE: You configure local authorization from **Role Based Access Control > Roles > Create Role** task. See [“Configuring Users to Manage Objects in Junos Space Overview” on page 521](#), [“Creating User Accounts” on page 571](#), and [“Creating a User-Defined Role” on page 553](#).

The following sections describe the authentication modes:

- [Local Authentication on page 758](#)
- [Remote Authentication on page 758](#)
- [Remote-Local Authentication on page 759](#)

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, use the **Role Based Access Control > User Accounts > Create User** (icon) task. To configure Junos Space Network Management Platform authentication, see [“Creating User Accounts” on page 571](#).

Remote Authentication

User authentication information is stored on one or more remote authorization servers. Authorization information can also be configured and stored on the remote authentication server. To configure Junos Space Network Management Platform remote authentication, see [“Configuring a RADIUS Server for Authentication and Authorization” on page 764](#).

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 can also be configured and stored on the remote authentication server. For more information about configuring a RADIUS server for the authentication and authorization of users, see [“Configuring a RADIUS Server for Authentication and Authorization” on page 764](#).

In this mode, when a user is not configured on the remote authentication server, when the server is unreachable, or when the remote server 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 757](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 764](#)
- [Configuring TACACS+ for Authentication and Authorization on page 768](#)
- [Managing Remote Authentication Servers on page 759](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)

Managing Remote Authentication Servers

The **Administration > Authentication Servers** 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 **Authentication Servers** page includes two areas: **Authentication Mode Setting** and **Remote Authentication Servers** table.

From the **Authentication Mode Setting** 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 > Authentication Servers**.
2. In the **Authentication Mode Setting** 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 Servers** 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 **Remote Authentication Servers** table, add a new remote authentication server by clicking the **Add auth server (+)** icon. See [“Creating a Remote Authentication Server” on page 760](#).
5. Modify an authentication server by doubling clicking that server row in the table. See [“Modifying Authentication Settings” on page 763](#).
6. Delete an authentication server by selecting a row and clicking the **Delete auth server (-)** icon 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 the server is at the top of the list; down arrow is disabled if the server is 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 that the server settings are correct.

Related Documentation

- [Remote Authentication Overview on page 757](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)
- [Junos Space Login Behavior with Remote Authentication Enabled on page 770](#)

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 > Authentication Servers**.
2. In the Authentication Mode Setting area, select the authentication method you want to use.

In local authentication mode, the controls for the Remote Authentication Servers 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 Remote Authentication Servers table, add a new remote authentication server by clicking the **Add auth server (+)** icon.

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 98 on page 761](#).

Table 98: Remote Authentication Server Settings

Setting	Description
Server Type	The type of the authentication server to be added. Choose RADIUS or TACACS+ depending on whether you want to authenticate the users using RADIUS or TACACS+ authentication server.
Server Name	The name of the server. The remote authentication server name cannot exceed 128 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.).
Protocol	The supported authentication protocols: <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 for the RADIUS server. RADIUS has been officially assigned UDP port 1812 for RADIUS Authentication. The default port number for the TACACS+ server is 49.

Table 98: Remote Authentication Server Settings (*continued*)

Setting	Description
Shared Secret	<p>The text string that serves as a password between the RADIUS server, proxy, and client.</p> <p>Enter the text string again in the Confirm Shared Secret field to confirm the shared secret or password.</p>
Number of Tries	<p>The number of retries that a device can attempt to contact a RADIUS authentication server. The default tries is 3 .</p> <p>You can enter a value from 1 through 5.</p>
Max Retry Timeout MSecs	<p>The interval in milliseconds that 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.</p> <p>The minimum value is 1000.</p>

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 Authentication 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 757](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Modifying Authentication Settings on page 763](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 764](#)

Modifying Authentication Settings

The 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. Select **Administration > Authentication Servers**.

The Authentication Servers page appears.

2. In the Authentication Mode Setting 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 Servers 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 Remote Authentication Servers table click the server edit icon that you want to modify. See [“Creating a Remote Authentication Server” on page 760](#).

The Modify Authentication Server dialog box appears.

5. 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 760](#).

6. In the Create Auth Server dialog box, click **OK**.

The modified remote authentication server settings are saved in the database.

7. On the Authentication 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 757](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Managing Remote Authentication Servers on page 759](#)
- [Junos Space Login Behavior with Remote Authentication Enabled on page 770](#)

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 > Authentication 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 597](#)).

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 > Authentication Servers**.
2. Under Authentication 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.

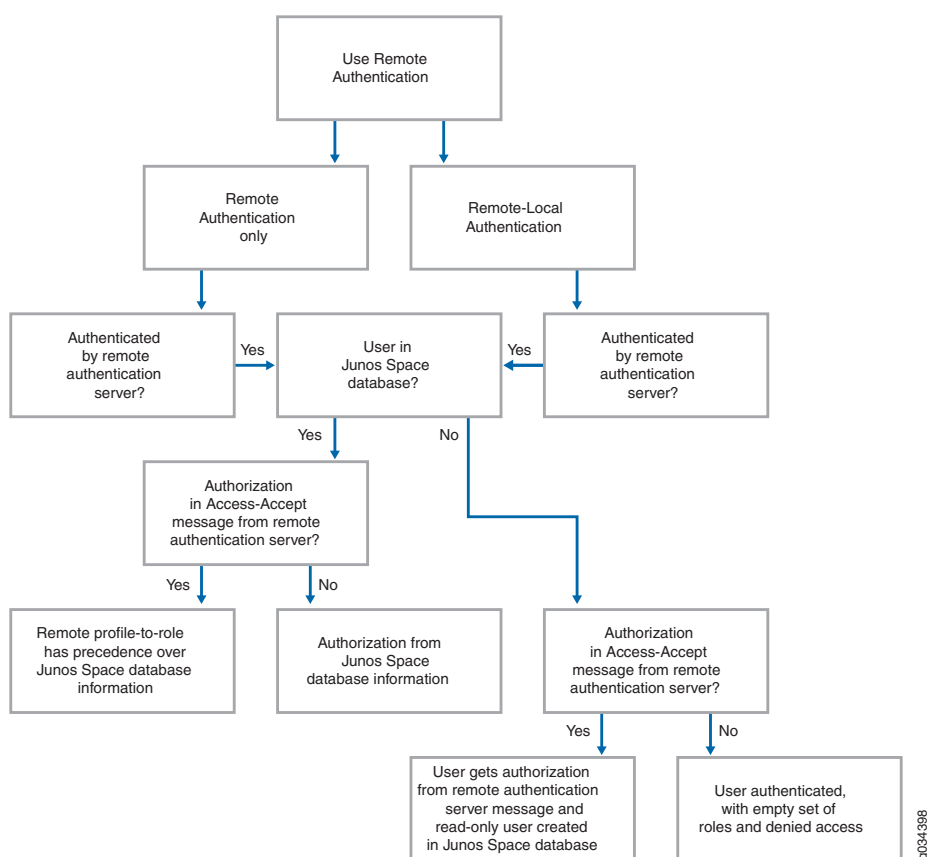
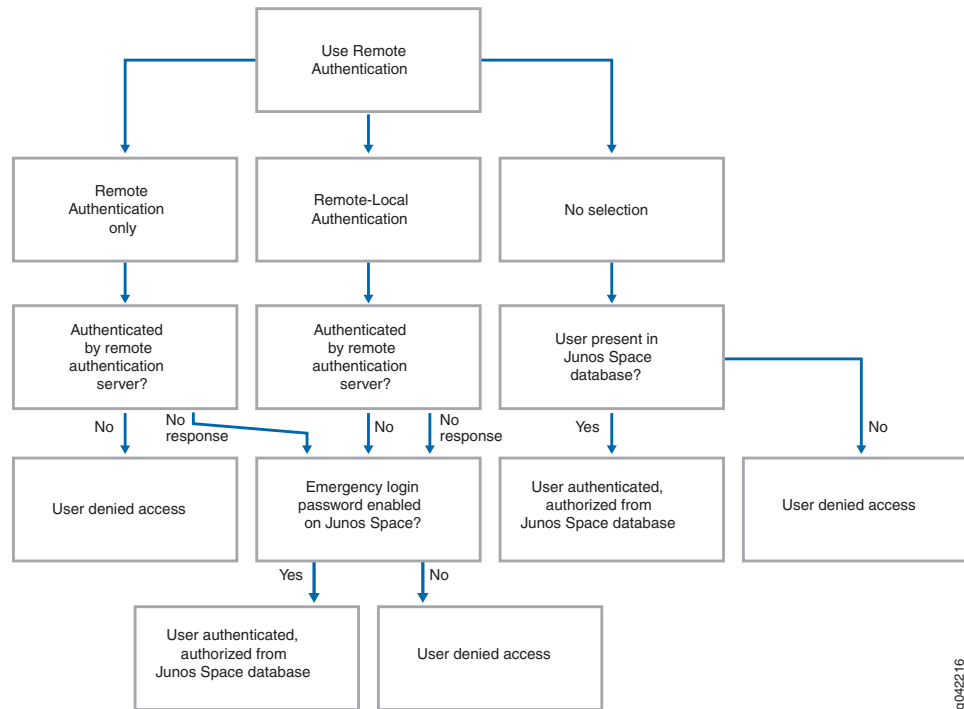


Figure 2 shows the results when a remote RADIUS server either rejects the user or does not respond at all.



g042216

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 (remote) 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 remote user to assign roles. This user is differentiated by a different icon on the Manage Users screen.

If any remote 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 remote 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 remote 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 remote users.)

**Related
Documentation**

- [Remote Authentication Overview on page 757](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Managing Remote Authentication Servers on page 759](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)
- [Configuring TACACS+ for Authentication and Authorization on page 768](#)
- [Junos Space Login Behavior with Remote Authentication Enabled on page 770](#)

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 > Authentication Servers**.
2. In the Authentication Mode Setting area, select the authentication method you want to use.

In local authentication mode, the controls for the Remote Authentication Servers 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 Remote Authentication Servers table, add a new remote authentication server by clicking the **Add auth server (+)** icon.

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 99 on page 768](#).

Table 99: 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	<p>The name of the server.</p> <p>The remote authentication server name cannot exceed 128 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.).</p>
Protocol	<p>The supported authentication protocols:</p> <ul style="list-style-type: none"> • PAP—Password Authentication Protocol • CHAP—Challenge Handshake Authentication Protocol

Table 99: TACACS+ Remote Authentication Server Settings (*continued*)

Setting	Description
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 TCP port number. The default is 49.
Shared Secret	The text string that serves as a password between the TACACS+ server, proxy, and client. Enter the text string again in the Confirm Shared Secret field to confirm the shared secret or password.
Number of Tries	The number of retries that a device can attempt to contact a TACACS+ authentication server. The default is 3 tries. You can enter a value from 1 through 5.
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. The minimum value is 1.

6. In the Create Auth Server dialog box, click **OK**.
7. In the Authentication 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 757](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Managing Remote Authentication Servers on page 759](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)
- [Configuring a RADIUS Server for Authentication and Authorization on page 764](#)
- [Junos Space Login Behavior with Remote Authentication Enabled on page 770](#)

Junos Space Login Behavior with Remote Authentication Enabled

This topic describes the Junos Space Network Management Platform login 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, login success or failure solely depends on the password stored there because no other servers are contacted. 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 (that is, whether a user is logging in with incorrect credentials or a user does not exist on the remote authentication server). Therefore, Junos Space Network Management Platform must always treat these type of logins as an authentication failure.

- 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, the user cannot log in to Junos Space Network Management Platform.
- The user attempts to log in but the remote server is down. See the previous two login 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 that 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 challenge question is answered correctly, it is possible that the authentication server may pose additional challenges questions.
 - If the challenge question is answered incorrectly, it is possible that the authentication server may rechallenge the user with the same challenge question, use a different challenge question, or fail the login attempt completely. The remote authentication server configuration determines the behavior.
 - If the final challenge is answered correctly, the user logs in successfully.

Login 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 through 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 the user locally. If a Junos Space Network Management Platform local password exists 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 the user locally. If a Junos Space Network Management Platform local password exists and the credentials match, the user logs in successfully.
- The user attempts to log in but the remote server is down. The user is authenticated using only the local password. If the password exists locally on the Junos Space server 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 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.
- The user attempts to log in when the remote authentication server is configured for Challenge/Response:
 - If the remote authentication server indicates that 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 the challenge question correctly, it is possible that the authentication server may pose additional challenges questions.
 - If the user answers the challenge question correctly, it is possible that the authentication server may rechallenge the user with the same challenge question, use a different challenge question, or fail the login attempt completely. The remote authentication server configuration determines the behavior.
 - If the user answers the challenge question correctly, the login is successful.



NOTE: When you configure the remote authentication server in the challenge–response mode, the authentication server poses one or more challenges (questions) to the user. The user is allowed to log in based on the responses of the user.

**Related
Documentation**

- [Remote Authentication Overview on page 757](#)
- [Logging In to Junos Space on page 3](#)
- [Junos Space Authentication Modes Overview on page 758](#)
- [Creating a Remote Authentication Server on page 760](#)
- [Modifying Authentication Settings on page 763](#)

Manage SMTP Servers

- [Managing SMTP Servers on page 775](#)
- [Adding an SMTP Server on page 776](#)

Managing 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 SMTP Servers page appears listing all the configured servers. Only one server 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 (**Add SMTP server** icon) at the upper left of the page to add a server.
2. Configure and add the server. See [“Adding an SMTP Server” on page 776](#).
3. To delete a server, click the – sign (**Delete SMTP server** icon) at the upper left of the page.



NOTE: If you try to delete the active SMTP server, an error message is displayed indicating that you cannot delete the server.

To change the active SMTP server:

- Click the **Set Active SMTP server** icon at the upper left of the page to select the server you want to make active. Click **Yes** on the confirmation message that appears to set the selected server as the active SMTP server. If there is only one server and it is the active server, clicking **No** on the confirmation message has no effect.

The Test connection settings option is used to test the SMTP server connection from Junos Space Network Management Platform. This option uses the user-defined (selected), 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 page.

If the SMTP server supports only the 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 776](#)

Adding an 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** text box, enter a name for the SMTP server, using alphanumeric values.

The SMTP server name cannot exceed 128 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.).

4. In the **Host Address** text box, enter the IP address or the hostname of the mail server.

The IP address or the hostname that you enter should be valid and should not contain any special characters.

5. Enter the port number in the **Port Number** text box

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

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

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

7. Select the **Set As Active Server** check box to set this server as the primary or active SMTP server. All applications then redirect the e-mail message to this SMTP server.
8. (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 fields are enabled.

9. (Optional) In the **User Name** text box, enter the username that you want to use for authentication.
10. (Optional) Enter the authentication password in the **Password** and **Confirm Password** text boxes.
11. (Optional) If you want to use Transportation Layer Security (a cryptographic protocol) or Secure Sockets Layer (SSL) for further protection, select **TLS** or **SSL** from the **Security** list.
12. Click **Save**.

Related Documentation

- [Managing SMTP Servers on page 775](#)

CHAPTER 74

Manage Tags

- [Tags Overview on page 779](#)
- [Managing Tags on page 781](#)
- [Creating Tags on page 798](#)

Tags Overview

- [Tags Overview on page 780](#)

Tags Overview

You can create user-defined tags on 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 the status or perform a bulk action on them without having to select each object individually.

The tags are classified into two categories: private tags and public tags. Private tags are those that are created by you and can be used only by you because they are not visible to others. Public tags are those that are available to all users for tagging objects that are accessible to them. You need the Tag Administrator role privileges to create, modify, or delete a public tag, manage hierarchical tags, as well as convert a private tag to a public tag. However, any Junos Space user can:

- Create, modify, and delete private tags
- View public and private tags
- Tag and untag objects by using public and private tags



NOTE: You cannot view or access private tags created by other users.

However, if you are a user with the Tag Administrator role, you can view and access private tags of other users.

Tag names should not start with a space, cannot contain a comma, double quotation marks, and parentheses, and cannot exceed 255 characters. Also, you cannot name a tag “Untagged” because it is a reserved term.

To use Tags:

1. Create a private or public (shared tag) by using the **Administration > Tags > Create Tag** user interface (see [“Creating a Tag” on page 798](#)), or from a Device Management or Job Management inventory landing page (see [“Managing Hierarchical Tags” on page 783](#)).
2. Tag an object on an inventory page. For example you can tag an object on the Device Management inventory page. After you tag an object, you can view or untag existing tags. See [“Tagging an Object” on page 793](#) and [“Untagging Objects” on page 794](#).
3. (Optional) Create hierarchical tags and manage them on the Tag Hierarchy pane in the Tag view on an inventory landing page for taggable objects (such as devices or jobs). See [“Managing Hierarchical Tags” on page 783](#).
4. Manage tags using the **Administration > Tags** inventory page, or a Device Management or Job Management inventory landing page. You can view, share, rename, or delete tags, as well as view the list of objects assigned to a tag from this page. See [“Viewing Tags for a Managed Object” on page 794](#), [“Sharing a Tag” on page 789](#), [“Renaming Tags” on page 790](#), [“Deleting Tags” on page 791](#), and [“Viewing Tagged Objects” on page 796](#).

- Related Documentation**
- [Tagging an Object on page 793](#)
 - [Untagging Objects on page 794](#)
 - [Filtering the Inventory by Using Tags on page 795](#)
 - [Viewing Tagged Objects on page 796](#)
 - [Managing Hierarchical Tags on page 783](#)

Managing Tags

- [Managing Tags on page 781](#)
- [Managing Hierarchical Tags on page 783](#)
- [Sharing a Tag on page 789](#)
- [Renaming Tags on page 790](#)
- [Deleting Tags on page 791](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)
- [Untagging Objects on page 794](#)
- [Filtering the Inventory by Using Tags on page 795](#)
- [Viewing Tagged Objects on page 796](#)

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 that you created. You must have the Super Administrator, System Administrator, or Tag Administrator role to manage tags.

The Tags page is empty for a new Junos Space installation until you create public and private tags. However, if you have upgraded from a previous release, then public and private tags from the preupgraded setup are listed on the Tags page. Tags are visible only to you unless the Tag Administrator shares them and makes them public to all users. Tags created by other users are private and visible only to them unless the Tag Administrator shares them and makes them public to all users.

You can manage all tags applied to inventory objects from the **Administration > Tags** inventory page. You can share, rename, or delete tags. You can view the list of objects assigned to a tag from the Tags page.

Viewing Tags

To view tags on the inventory page:

- All tags appear on the inventory page in tabular view and are listed alphabetically by tag name.

You can filter inventory objects by tag name (see [“Filtering the Inventory by Using Tags” on page 795](#)).

Viewing Tag Information

Tag data includes tag name, tag owner, access type, and number of objects tagged by a particular tag. See [Table 100 on page 782](#).

Table 100: Tag Information

Tag Data	Description
Name	Unique tag name. Tag names cannot start with a space or be longer than 256 characters.
Owner	<p>Owner of a private tag. Public tags do not have a specific owner and hence this column is empty for public tags.</p> <p>A user with the Super Administrator role can view private tags of all users, whereas a user without this role can view only the private tags created by that user.</p>
Access Type	Tags can be public (shared) or private (visible only to the creator).
Tagged Object Count	Number of objects tagged in all workspace inventory pages by the tag. You can click the link to view the objects that are assigned to a specific tag.

You can sort and hide columns. You can also filter data on the Name, Owner, and Access Type columns. For more information about manipulating tables in tabular view, see *Junos Space User Interface Overview* in the *Junos Space User Interface Guide*.

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 the shortcut menu.

You can share (see [“Sharing a Tag” on page 789](#)), rename (see [“Renaming Tags” on page 790](#)), delete (see [“Deleting Tags” on page 791](#)), or deselect all selected tags. You can also view the objects that are assigned the selected tag ([“Viewing Tagged Objects” on page 796](#)).

Related Documentation

- [Tags Overview on page 780](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)

- [Untagging Objects on page 794](#)
- [Creating a Tag on page 798](#)

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.



NOTE: Only public tags can be hierarchical. That is, you can create a public tag within another public tag.

You can view, create, update, and delete hierarchical tags on the **Devices > Device Management** inventory page and **Jobs > Job Management** inventory page. For more information about creating, modifying, and deleting tags, see [“Using the Shortcut Menu” on page 785](#). This topic contains information about working with tags on the Device Management page. You can extend this information to the Job Management page.

The **Devices > Device Management** inventory page displays all devices on the network that are accessible to you and that are managed by Junos Space Network Management Platform. To filter devices on the basis of tags:

1. Click the **Display Tag View** icon on the toolbar.

The Tag Hierarchy pane appears, which displays a tree view of all tags (public and private tags) that are relevant to the inventory landing page that you are currently on.

You can view, create, update, and delete tags on this pane.

2. Mouse over a tag to view the number of objects assigned to a public or private tag.

The Tag Hierarchy pane also displays the **Untagged** category, which lists the number of devices that are not tagged.

3. Select a public or private tag on the tag hierarchy tree to filter devices that are assigned the selected tag. The devices tagged assigned with this specific tag appear in a tabular view (also called Tabular View Pane).

If you click **Untagged**, the devices that are untagged are displayed.

- [Using the Tag Hierarchy Pane on page 784](#)
- [Using the Tabular View Pane on page 788](#)

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 **Display Tag View** icon on the **Devices > Devices Management** inventory page.

- [Using the Tag Action Bar on page 784](#)
- [Using the Shortcut Menu on page 785](#)
- [Using Drag-and-Drop on page 787](#)
- [Using the Quick Info Tool Tip on page 787](#)
- [Browsing Tagged Objects on page 788](#)
- [Viewing All Tags on page 788](#)
- [Adding a Child Tag on page 788](#)
- [Deleting a Tag on page 788](#)
- [Using Notification on page 788](#)

Using the Tag Action Bar

You can use the Tag Action bar to add a 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.



NOTE: Only public tags can be hierarchical. That is, you can create a public tag within another public tag.

To add a public or private tag:

1. Select the **Public** or **Private** category depending on the type of tag that you want to add.
2. Click the **Add Tag** (plus [+] button) on the Tag Action bar. This option is disabled if you do not have the necessary permissions.

The Create Tag dialog box appears.

3. Type a new tag name in the **Tag Name** field.

If you are adding a new tag, ensure that the tag name does not:

- Exceed 255 characters
- Start with a space
- Contain special characters, such as commas, double quotation marks, and parentheses



NOTE: “Untagged” is a reserved term and hence you cannot create a tag with this name.

4. Select the **Make Public** check box.

If you do not select this check box, then a private tag is created.

5. Click the **Add Tag** button.

A new tag is added to the tag hierarchy.

To delete a tag:

1. Select the tag you want to delete from the tag hierarchy tree.
2. Click the **Delete Tag** (minus [–] button) on the Tag Action bar. This option is disabled if you do not have the necessary permissions.

A confirmation dialog box appears.



NOTE: If you are deleting a child tag and you want to remove the child tag completely from Junos Space Network Management Platform, select the **Also delete <tag-name> tags** check box on the confirmation dialog box. If this check box is not selected and if the selected tag appears in multiple locations, then it is deleted from the current location only.



CAUTION: If you have assigned this tag to any object, then the object-tag association is lost when you click Yes on the confirmation dialog box.

3. Click **Yes** to delete the tag.



NOTE: The tag is deleted and any object-tag association is lost. However, you can click No on the confirmation dialog box to prevent this and the tag is not deleted.

Using the Shortcut Menu

When you right-click a tag in the tag hierarchy tree, a shortcut 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 in case of a public tag or to add a new private tag. Use **Modify Tag** and **Remove Tag** options to modify and delete a tag, respectively.



NOTE: Only public tags can be hierarchical. That is, you can create a public tag within another public tag.

To add a child tag by using the shortcut menu:

1. Right-click a public tag in the tag hierarchy tree for which you want to add a child tag.

The shortcut menu appears.

2. Click the **Add Tag** option on the shortcut menu. This option is disabled if you do not have the necessary permissions.

The Create Tag dialog box appears.

3. Type a new tag name in the field.

If you are adding a new tag, ensure that the tag name does not:

- Exceed 255 characters
- Start with a space
- Contain special characters, such as commas, double quotation marks, and parentheses



NOTE: “Untagged” is a reserved term and hence you cannot create a tag with this name.

4. Click the **Add Tag** button.

A new child tag is added to the tag hierarchy.

To modify a tag by using the shortcut menu:

1. Select the tag you want to modify from the tag hierarchy tree.
2. Click the **Modify Tag** option on the shortcut menu. This option is disabled if you do not have the necessary permissions.

The Edit Tag Name or Description dialog box appears.

3. Edit the tag name or the description, as needed.
4. Click **Modify Tag** to modify the tag.



NOTE: If you have assigned this tag to any object, then those objects are associated with the modified tag.

To delete a tag by using the shortcut menu:

1. Select the tag you want to delete in the tag hierarchy tree.
2. Click the **Delete Tag** option on the shortcut menu. This option is disabled if you do not have the necessary permissions.

A confirmation dialog box appears.



NOTE: If you are deleting a child tag and you want to remove the child tag completely from Junos Space Network Management Platform, select the **Also delete <tag-name> tags** check box on the confirmation dialog box. If this check box is not selected and if the selected tag appears in multiple locations, then it is deleted from the current location only.



CAUTION: If you have assigned this tag to any object, then the object-tag association is lost when you click **Yes** on the confirmation dialog box.

3. Click **Yes** to delete the tag.



NOTE: The tag is deleted and any object-tag association is lost. However, you can click **No** on the confirmation dialog box to prevent this and the tag is not deleted.

Using Drag-and-Drop

You can drag a public 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.

When you try to drag a public tag from one location to another, you can either move the tag from the current location to another location or copy the tag. The copy operation is used to make an identical copy of the tag in the new location, whereas the move operation is used to move the tag from the current location to a new location.



NOTE: You can move tags only within the public tags hierarchy. If you do not have permissions to create or delete tags, you cannot move tags.

Using the Quick Info Tool Tip

The Quick Info tool tip provides quick and immediate statistics about a tag. You can place the cursor over a tag name or a tag icon in the tag hierarchy tree to see a quick summary of its tagged objects.

To view the tool tip for a tag:

1. Select a particular tag in the tag hierarchy tree.
2. Place the cursor 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 **Device Management** inventory page only. In this mode, only those tags appear that are either empty or a tag that has at least one object on the inventory page. This is because **Show Relevant Tags** is selected by default on the **Tags** list located at the top of the Tag Hierarchy pane.

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 shortcut menu to add a child tag to the tag hierarchy tree. To add a child tag by using the Tag Action bar, see [“Using the Tag Action Bar” on page 784](#). To add a child tag by using the shortcut menu, see [“Using the Shortcut Menu” on page 785](#).

Deleting a Tag

You can use either the Tag Action bar or the shortcut menu to delete a tag from the tag hierarchy tree. To delete a tag by using the Tag Action bar, see [“Using the Tag Action Bar” on page 784](#). To delete a tag by using the shortcut menu, see [“Using the Shortcut Menu” on page 785](#).

Using Notification

When multiple Junos Space Network Management Platform users view the same tag view on the **Device Management** 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 by 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 about how to tag an object, see [“Tagging an Object” on page 793](#).

To search for specific tagged objects:

1. Navigate to the Device Management page.
2. Select a tag in the search box.

The tag hierarchy tree navigates to the selected tag, and the Tabular View pane displays the objects that are tagged with that particular tag only.

Related Documentation

- [Tags Overview on page 780](#)

Sharing a Tag

User-defined tags are always created as private tags initially. If your tag has public value, you can share it to make it public for all users to tag objects on a workspace inventory page. To share a tag, you must have Tag Administrator privileges.

To share a tag.

1. On the Junos Space Network Management Platform user interface, select **Administration > Tags**.

The **Tags** inventory page appears.

2. Select one or more private tags on the inventory page. The **private** keyword in the **Access Type** column on the Tags page indicates private tags.
3. Select **Make Tag Public** from the Actions menu or the shortcut menu.

The **Share Tag** status box indicates whether you have shared the tag successfully.

You can also share a tag when you add a new tag. (see [“Creating a Tag” on page 798](#)).

4. Click **OK** on the Share Tag status box.

The **Access Type** of the tag changes on the inventory table from **private** to **public**.



NOTE: You cannot revert a public tag to a private tag.

When you share a tag, an audit log entry is automatically generated.

Related Documentation

- [Tags Overview on page 780](#)
- [Managing Tags on page 781](#)
- [Renaming Tags on page 790](#)
- [Deleting Tags on page 791](#)
- [Creating a Tag on page 798](#)

Renaming Tags

The Modify Tag command enables you to reorganize or recategorize managed objects according to your changing needs.

To rename a tag:

1. On the Junos Space Network Management user interface, select **Administration > Tags**.

The Tags inventory page appears.

2. Select the tag that you want to rename.
3. Select **Modify Tag** from the shortcut menu.

The **Modify Tag** dialog box appears.

4. Type a tag name in the **New Name** field.

A tag name should not start with a space, cannot contain a comma, double quotation marks, and parentheses, or exceed 255 characters. Also, "Untagged" is a reserved term and hence you cannot have a tag with this name.

5. Click **Modify**.

The old tag is renamed and saved in the database. You see the renamed tag on the inventory page. The objects that were associated with the old tag are now associated with the modified tag.

You can rename a tag not only from the Tags workspace but also from other workspaces such as the Device Management inventory landing page or the Job Management inventory landing page.

To rename a tag from the Device Management inventory landing page:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. If tags are not displayed, click the **Display Tag View** icon on the toolbar.
3. Select a tag and click **Modify Tag** from the shortcut menu.
4. Type a tag name in the **Tag Name** field.

A tag name should not start with a space, cannot contain a comma, double quotation marks, and parentheses, or exceed 255 characters. Also, "Untagged" is a reserved term and hence you cannot have a tag with this name.

5. Modify the description in the **Description** field.
6. Click **Modify**.

The old tag is renamed and saved in the database. You see the renamed tag on the inventory page. The objects that were associated with the old tag are now associated with the modified tag.

When you modify a tag, an audit log entry is automatically generated.

Related Documentation

- [Tags Overview on page 780](#)
- [Managing Tags on page 781](#)
- [Sharing a Tag on page 789](#)
- [Deleting Tags on page 791](#)
- [Creating a Tag on page 798](#)
- [Filtering the Inventory by Using Tags on page 795.](#)

Deleting Tags

Use Delete Tags to remove tags that you no longer need.



NOTE:

- You can delete a public tag only if you have sufficient permissions. Contact your system administrator if this need arises.
- Private tags created by other users are not visible to you and hence you cannot delete them. Even a user with the Tag Administrator role is not permitted to delete private tags of other users.

You can delete your private tags not only from the Tags inventory page but also from any inventory page where deletion of private tags is permitted. Select **Delete Private Tags** from the Actions menu on the respective inventory landing page.

- You cannot delete the top-level **Public**, **Private**, or **Untagged** categories. You can delete the tags only within the **Public** and **Private** categories.

To delete a public or a private tag from the Tags workspace:

1. On the Junos Space Network Management Platform user interface, select **Administration > Tags**.

The **Tags** page appears.

2. Select one or more tags that you want to delete.
3. Select **Delete Tags** from the shortcut menu.

This option is disabled if you do not have sufficient permissions to delete the selected tags. This situation may arise when you are trying to delete a public tag for which you do not have the necessary permissions. Contact your system administrator for this task.

The **Delete Tags** dialog box appears to confirm that you want to delete the tag.

4. Click **Delete** on the confirmation dialog box.

The tag is removed from the database and no longer appears on the Tags page.



CAUTION: If you have assigned a tag that you are deleting with any object, no warning message is displayed before the deletion of the tag. When you delete a tag, Junos Space Network Management Platform removes the object-tag association and the tag is no longer associated with any object. The deletion of a tag does not delete any tagged objects.

You can delete a tag not only from the Tags workspace but also from other workspaces such as the Device Management inventory landing page or the Job Management page.

To delete a tag from the Device Management inventory landing page:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page appears.

2. If tags are not displayed, click the **Display Tag View** icon on the toolbar.
3. Select a tag and click **Delete Tag** from the shortcut menu.

This option is disabled if you do not have sufficient permissions to delete the selected tags. This situation may arise when you are trying to delete a public tag for which you do not have the necessary permissions. Contact your system administrator for this task.

A confirmation dialog box appears to confirm whether you want to delete the tag.

4. Click **Yes** on the confirmation dialog box.

The tag is removed from the database and no longer appears on the Tags page.



CAUTION: If you have assigned the tag that you are deleting to any object, no warning message is displayed before the deletion of the tag. When you delete a tag, Junos Space Network Management Platform removes the object-tag association and the tag is no longer associated with any object. The deletion of the tag does not delete any tagged objects.

When you delete a tag, an audit log entry is automatically generated.

**Related
Documentation**

- [Tags Overview on page 780](#)
- [Managing Tags on page 781](#)
- [Sharing a Tag on page 789](#)
- [Renaming Tags on page 790](#)
- [Creating a Tag on page 798](#)

Tagging an Object

You can create user-defined tags on 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 the status or perform a bulk action on them without having to select each object individually.

By default, the tags that you create from any workspace are private tags and these private tags are visible only to you. If you want any other user to use the tag that you created, then you have to create a public tag instead of a private tag or convert the private tag to a public tag.

To tag an object:

1. Navigate to an application workspace manage inventory page. For example, select **Devices > Device Management**.
2. Select the inventory objects that 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 field.

If you have existing tags, start to type a tag name in the name field. Existing tags appear in the selection box.

You can also type a new tag name in the field. The new tag is automatically created and applied to the selected objects.

5. (Optional) Select the **Make Public** check box to mark the new tag created in the previous step as a public tag. If you do not select this check box, the new tag added is classified as a private tag.



NOTE: If you do not have permissions to create a public tag, then the **Make Public** check box is disabled.

6. (Optional) Add a comment in the **Add Description here** field.
7. Click **Apply Tag**. This action tags the object and stores the tag in the database.

Related Documentation

- [Tags Overview on page 780](#)
- [Managing Tags on page 781](#)
- [Viewing Tags for a Managed Object on page 794](#)
- [Untagging Objects on page 794](#)
- [Filtering the Inventory by Using Tags on page 795](#)
- [Creating a Tag on page 798](#)

Viewing Tags for a Managed Object

The View Tags action from application workspace inventory pages allows you to see all tags that you have assigned to 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 individually.

Tags created by you are private and visible only to you unless you have the Tag Administrator share them to the public domain, making them public. Tags created by other users are visible only to them unless the Tag Administrator shares them, then including 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**.

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 781](#)
- [Tagging an Object on page 793](#)
- [Untagging Objects on page 794](#)

Untagging Objects

You can untag or remove a tag from an object on a workspace inventory page. You can select only 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** from the Actions menu or right-click an object and select **UnTag It** from the shortcut 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 780](#)
- [Managing Tags on page 781](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)
- [Creating a Tag on page 798](#)

Filtering the Inventory by 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 to categorize by tag name.

To filter the inventory by 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 on the search field.

A list appears with object names at the top and tag names at the bottom. (If you typed a letter in the search field, only the tag names starting with that letter appear.)

2. Click a tag name on 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 preview the tagged objects that 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 780](#)
- [Managing Tags on page 781](#)
- [Tagging an Object on page 793](#)
- [Viewing Tags for a Managed Object on page 794](#)
- [Untagging Objects on page 794](#)
- [Creating a Tag on page 798](#)

Viewing Tagged Objects

You can click the **View Tagged Objects** task from the Tags workspace to view the list of objects that are assigned to a tag.

You do not need the Tag Administrator privileges to view this information. Any user has access to this information.

To view objects that are associated with a specific tag:

1. On the Junos Space Network Management Platform user interface, select **Administration > Tags**.

The Tags page appears, displaying the following columns:

- **Name**—Name of the tag
- **Owner**—User who owns or created the tag. Owners are displayed only for private tags. For a public tag, this column is empty.
- **Access Type**—Whether the tag is a private or public tag
- **Tagged Object Count**—Number of objects that are associated with a specific tag.

2. Perform one of the following tasks to open the View Tagged Objects page:

- Select a tag and from the Actions menu, select **View Tagged Objects**.

The View Tagged Objects page appears.

- Select and right-click a tag, and from the shortcut menu, select **View Tagged Objects**.

The View Tagged Objects page appears.

- Click the hyperlink on the **Tagged Object Count** column for a specific tag.

The View Tagged Objects page appears.



NOTE: The View Tagged Objects page is divided into two panes. The left pane displays the category and the right pane displays the objects that are tagged in the selected category. Objects listed in the Category column are sorted alphabetically.

This page is read-only. No actions are permitted on this page.

If no objects are tagged, then the **View Tagged Objects** task is disabled on the Action and shortcut menus, and the tagged object count displays a count of 0 and is not hyperlinked.

3. Select a category on the left pane to view the objects that are associated with the selected category. For example, to view the objects that are tagged in the script category, select **Script** on the left pane. The right pane displays the scripts that are tagged by using the specific tag along with their names and descriptions.

The total object count for the selected category is displayed at the top of the View Tagged Objects page. When the object count is high, use the **Show items** list to manage the number of objects that are displayed and the paging controls to navigate to a specific page. These controls are available at the bottom of the View Tagged Objects page. You can also sort and filter data in the **Name** column to quickly locate any information.



NOTE: Only supported objects are displayed on the right pane. When you click a category that has tagged unsupported objects, the following error message is thrown:

Object information is not available for this category.

For a list of objects that are supported, see [Table 101 on page 797](#).

4. To return to the Tags page, click **Back** on the upper left of the View Tagged Objects page.

Table 101: Objects Supported on the View Tagged Objects Page

Category or Workspace	Object Types	Objects
Device Management	Devices	Name —Hostname of the device
		IP Address —IP address of the device
	Deployment instances	Name —Name of the deployment instance
		Description —Description of the deployment instance
Images and Scripts	Scripts	Name —Name of the script
		Description —Description of the script
	Images	Name —Name of the image
		Description —Description of the image
	Operations	Name —Name of the operation
		Description —Description of the operation
	Script Bundle	Name —Name of the script bundle
		Description —Description of the script bundle

Table 101: Objects Supported on the View Tagged Objects Page (*continued*)

Category or Workspace	Object Types	Objects
Device Templates	Template definitions	Name —Name of the template definition
		Description —Description of the template definition
	Templates	Name —Name of the template
		Description —Description of the template
CLI Configlets	Configlets	Name —Name of the configlet
		Description —Description of the configlet
Report Management	Report Definition	Name —Name of the report definition
		Description —Description of the report definition
	Generated Reports	Name —Name of the generated report
		Description —Description of the generated report
Job Management		Jobs —Name of the job
		Description —Owner and state of the job
Role Based Access Control	User Accounts	Username —Name of the user
		Description —First name and last name of the user
	Roles	Name —Name of the role
		Description —Description of the role

- Related Documentation**
- [Tagging an Object on page 793](#)
 - [Tags Overview on page 780](#)

Creating Tags

- [Creating a Tag on page 798](#)

Creating a Tag

You create tags when you want to label and categorize Junos Space Network Management Platform objects so that you can filter, monitor, or perform batch actions on them without having to select each object individually. All users can create their own private tags from

the Administration > Tags inventory landing page. However, users assigned the Tag Administrator role can create public tags.

You can create tags from the Administration workspace as well as from the Device Management or Job Management inventory landing page. By default, the tags that any user creates are private tags, which means that these tags are visible only to the user who creates them. No other user can access the private tags created by other users. However, if you are a user with the Tag Administrator role, you can make these tags public, thereby allowing all users to associate objects with these tags.

To create a tag from the Administration workspace:

1. On the Junos Space Network Management Platform user interface, select **Administration > Tags**.

The Tags page appears.

2. On the toolbar, click the **Create Tag** icon.

The **Create Tag** dialog box appears.

3. If necessary, select the **Share this Tag** check box.

When you share a tag, all users can use that tag. Only users with the Tag Administrator role can publish tags to the public domain. For users without this role, the **Share this Tag** check box is disabled (grayed out).

4. In the **Tag Name** field, type a tag name.

A tag name should not:

- Exceed 255 characters
- Start with a space
- Contain special characters, such as commas, double quotation marks, and parentheses.



NOTE: “Untagged” is a reserved term and hence you cannot create a tag with this name.

5. Click **Create**.

The Create Tag dialog box appears, displaying that the tag is successfully created.

6. Click **OK** on the Create Tag dialog box.

The newly added tag appears on the Tags page. If the tag is shared, it is public; if not, it is private. The **Access Type** column displays whether the tag is public or private.

In addition to creating tags from the Administration workspace, you can create tags from the following inventory landing pages as well:

- Device Management
- Job Management

For example, to create a tag from the Device Management inventory landing page:

1. On the Junos Space Network Management Platform user interface, click **Devices** > **Device Management**.

The Device Management page appears.

2. If the tags are not displayed, click the **Display Tag View** icon on the toolbar located at the top of this page.

On the left side of the page, tags that are relevant to the page and the domain to which you are logged in are displayed.



NOTE: Tags from domains other than the domain to which the user is logged in are not displayed.

In Tags View, the tags are categorized as follows:

- **Public**—Lists public tags. Public tags are tags that are visible and available to all users and can be used by any user to tag an object in Junos Space.

You can perform the following actions on public tags:

- Mouse over a tag to view the number of objects that are associated with the specific tag.
- Click a tag to view the devices associated with the selected tag. The number displayed adjacent to the tag shows the number of devices associated with the specific tag. For example, if you have assigned this tag to two devices, then the number displayed is 2. However, this rule has the following exceptions:
 - For hierarchical tags, the count on the parent tag does not include the number of objects associated with its child tags. For example, if a child tag is associated with 10 objects and its parent tag is associated with five objects, then the count displayed for the parent tag is 5 and not 15.
 - You used the same tag on objects other than devices. For example, if you assigned TagC to UserA and DeviceB, then on the Device Management page, the count shown for TagC is 1. However, when you mouse over TagC, the tooltip displays a count of 2 (which includes the object type as well—in this example, the object types that are displayed are **User** and **Device**).
- **Private**—Lists private tags. Private tags are tags that you created and hence are visible only to you. No other user has access to these tags.

Click a tag to view the devices associated with the selected tag. The number displayed adjacent to the tag shows the number of devices that are associated with the specific tag. For example, if you assigned this tag to two devices, then the number displayed is 2.

- **Untagged**—Displays the number of devices that are not tagged

3. (Optional) To view all tags (that is, tags that are relevant and irrelevant to the inventory landing page to which you are currently logged in), select **Show All Tags** on the **Tags** list at the top of the Device Management inventory landing page.

By default, **Show Relevant Tags** is selected and only the tags that are relevant to the current inventory landing page are displayed.

4. To add a tag:

- a. Click the **Add Tag** icon.



NOTE: If you use the shortcut menu instead of the Add Tag icon, the new tag that is added is of the same type as that of the parent. For example, right-click **Private** and select **Add Tag** to create a private tag.

- b. In the **Tag Name** field, type a tag name.

A tag name should not:

- Exceed 255 characters
- Start with a space
- Contain special characters such as commas, double quotation marks, and parentheses



NOTE: "Untagged" is a reserved term and hence you cannot create a tag with this name.

- c. If necessary, select the **Make Public** check box to create a public tag. If left unselected, a private tag is created.

When you make a tag public, all users can use that tag. Only the Tag Administrator can publish tags to the public domain.



NOTE: This check box is disabled if you chose to create a tag by using the shortcut menu. The new tag that is added is of the same type as that of the parent.

- d. (Optional) In the **Description** field, add a description of the tag.

- e. Click **Add Tag**.

The tag is added to the relevant tag category and assigned to the domain to which you are currently logged in. For example, if you created a public tag, the newly added tag is placed in the **Public** category. The count is set to zero (0) because you have not assigned this tag to any object.



NOTE: You cannot add any tags to the Untagged category.

When you add a tag, an audit log entry is automatically generated.

**Related
Documentation**

- [Tags Overview on page 780](#)
- [Managing Tags on page 781](#)
- [Sharing a Tag on page 789](#)
- [Renaming Tags on page 790](#)
- [Deleting Tags on page 791](#)

CHAPTER 75

Manage DMI Schemas

- [Managing DMI Schemas Overview on page 804](#)
- [Updating a DMI Schema on page 806](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 809](#)
- [Setting a Default DMI Schema on page 813](#)
- [Troubleshooting DMI Schema Management on page 814](#)

Managing DMI Schemas Overview

To manage multiple DMI schemas (device management interface schemas) for Junos OS-based device families and device types, use the DMI Schemas workspace.

Each device type is described by a unique data model (DM) that contains all the configuration data for the device. 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 is applied when you try to edit a device configuration by using the device configuration edit action in the Devices workspace (see [“Modifying the Configuration on the Device” on page 21](#)). If Junos Space Network Management Platform has exactly the right DMI schema for each of your devices, you can access all configuration options specific to each device.

The DMI Schemas workspace enables you to add or update schemas for all Junos Space devices.

You must set a default DMI schema for each device family. When you create a device template, the template requires a default schema for the device family. Conversely, to access all configuration options for a particular device through the Edit Device Configuration action on the Devices workspace, you must have the DMI schema specific to that device.

The schema management facility enables you to connect with the SVN Repository of Juniper Networks 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 as a .tgz file, which is an archive containing multiple files reflecting the configuration hierarchy for the selected device family, platform, and OS version. You can also create your own .tgz file (see [“Creating a Compressed Tar File for Updating DMI Schema” on page 809](#)).

Using the DMI Schemas workspace, you should be able to manage a device in Junos Space Network Management Platform.

For each DMI schema currently installed, the **DMI Schemas** inventory landing page displays the following columns:

- Device Family
- OS Version
- Device Series
- State

You can view the schemas in tabular form, and you can sort the schemas by clicking their column headings.

You can select one or more schemas and perform the following actions on them by using the shortcut menu:

- **View Schema Details**—View the details of the selected schema, such as its name, device series, device family, OS version, and state.
- **View Missing Schemas**—View the missing schemas.
- **Set Default Schema**—Perform this step to return a custom configuration of a DMI schema to its default setting.
- **Tag and untag schemas**—Use the Tags feature to label and categorize the schemas.
- **View Tags**—Select a schema and view all the tags associated with that schema. The View Tags page displays the tags with the following information:
 - **Tag Name**—Name of the tag
 - **Access Type**—Whether the tag is public or private

To add or update a DMI schema, see [“Updating a DMI Schema” on page 806](#).

**Related
Documentation**

- [Updating a DMI Schema on page 806](#)
- [Setting a Default DMI Schema on page 813](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 809](#)
- [Troubleshooting DMI Schema Management on page 814](#)
- [Device Discovery Overview on page 109](#)

Updating a DMI Schema

To add or update a DMI schema, you must have the .tgz archive containing the DMI schema 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 809](#)).
- Download a file from Juniper Networks' SVN repository. This topic contains instructions for doing this.
- Get a file from the Juniper Networks 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.

On the **Schema Update** page, you can perform one of the following tasks:

- Install a DMI schema on Junos Space Network Management Platform using a file you already have on the machine running the Junos Space GUI.
- Obtain a DMI schema from Juniper Networks and update Junos Space Network Management Platform, which involves the following subtasks:
 - 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 click 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 box appears.

3. Select the .tgz file and click **Open**.

The **Update Schema** page reappears, displaying the .tgz filename in the **Browse** field.

4. Click **Upload**.

Do not move away from the **Update Schema** page while the .tgz file is being uploaded to Junos Space Network Management Platform. Note that the process can take some time, depending on how many schemas are in the file.

5. (Optional) To overwrite a previously existing schema, select the **Enable Schema Overwrite** check box.
6. (Optional) To display the recommended schemas only, select the **Show recommended schemas only** check box.
7. Select the desired schema and click **Install**.

The **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. In a web browser, enter the following URL: <https://xml.juniper.net/dmi/repository/trunk>
You are prompted to enter the login credentials.
2. In the **User name** field, enter the username.
3. In the **Password** field, enter the password.
4. Select the **SVN Repository** option button.
5. Click **Configure**.

The **SVN Access Configuration** dialog box appears.

6. Enter the SVN URL, the username and the password in the appropriate text fields. Reenter the password and click **Test Connection**.

A message appears to indicate whether the connection is established successfully or not.

7. Whether or not the connection is successful, click **OK**.

The **SVN Access Configuration** dialog box reappears.

8. Perform one of the following steps:
 - If the connection failed, click **Cancel**, find the correct credentials, and repeat the preceding steps.
 - If the connection is 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 that the repository's URL appears in the URL field. If the field is blank, you must configure the connection. See step 5 above.
3. Click **Connect**.

The content of the repository with DMI schema releases appears in table form under **Available Updates** on the **Update Schema** page. The already installed versions are selected by default.

Junos Space Network Management Platform detects and marks 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.

Click on the column headings to sort the data by device family, release, or 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 only** 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 813](#).

Click **Install**.

A message appears, prompting you to wait. After the DMI schema is installed, the **DMI Schemas** page reappears, displaying the new schema.

**Related
Documentation**

- [Managing DMI Schemas Overview on page 804](#)
- [Setting a Default DMI Schema on page 813](#)
- [Troubleshooting DMI Schema Management on page 814](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 809](#)

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 806](#)).



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 [Installing Subversion](#) 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 102 on page 810](#).

Table 102: 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: <https://tortoisesvn.net/>.



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: <http://www.7-zip.org/>.



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 102 on page 810](#) 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.

[Table 103 on page 812](#) displays information about the schemas available for use in Junos Space Network Management Platform.

Table 103: Schema Name Mapping Information

Schema Family	Device Family Series	Examples of Supported Hardware in the Device Family
junos	ACX Series/J Series/M Series/MX Series/T Series/TX Series/PTX Series/EX92xx Series	ACX1000, ACX1100, ACX2000, ACX2100, ACX2200, ACX4000, EX9204, EX9208, EX9214, J2320 (ROUTING), J2350 (ROUTING), J4350 (ROUTING), J6350 (ROUTING), M10, M10I, M120, M20, M320, M40E, M7I, MX10, MX2010, MX2020, MX240, MX480, MX5, MX80-48T, MX960, PTX5000, T1600, T320, T4000, T640, TX-MATRIX, TX-MATRIX-PLUS
junos-es	J Series/SRX Series/LN Series	J2320 (SECURITY), J2350 (SECURITY), J4350 (SECURITY), J6350 (SECURITY), LN2600, SRX100, SRX100-HM, SRX100-LM, SRX100-VDSL-HM, SRX100-VDSL-LM, SRX100-WL-HM, SRX100-WL-LM, SRX100-WL-VDSL-HM, SRX100B, SRX100B-VDSL, SRX100B-WL, SRX100H, SRX100H-VDSL, SRX100H-WL, SRX100H-WL-VDSL, SRX110, SRX110H-VA, SRX110H-VB, SRX100H2, SRX110H2-VA, SRX110H2-VB, SRX1400, SRX210-HM, SRX210-LM, SRX210-POE, SRX210B, SRX210H, SRX210H-P-M, SRX210H-POE, SRX210HE2, SRX210HE2-POE, SRX220, SRX220H2, SRX220H2-POE, SRX240-HM, SRX240-LM, SRX240-POE, SRX240B, SRX240B2, SRX240H, SRX240H-P-M, SRX240H-POE, SRX240H2, SRX240H2-DC, SRX240H2-POE, SRX3400, SRX3600, SRX5600, SRX5800, SRX650
junos-ex	EX Series	EX-XRE, EX2200-12P-2G, EX2200-12T-2G, EX2200-24P-4G, EX2200-24T-4G, EX2200-48P-4G, EX2200-48T-4G, EX3200-24P, EX3200-24T, EX3200-48P, EX3200-48T, EX3300-24T, EX3300-48P, EX4200-24F, EX4200-24P, EX4200-24PX, EX4200-24T, EX4200-48P, EX4200-48PX, EX4200-48T, EX4200-VC, EX4300-24P, EX4300-24PX, EX4300-24T, EX4300-48P, EX4300-48PX, EX4300-48T, EX4300-VC, EX4500-40F, EX4500-40F-VC, EX4550-32F, EX4550-32F-VC, EX4550-32T, EX4550-32T-VC, EX6210, EX8208, EX8216
screenos	NS/SSG	NS204, NS208, NS50, NS500, NS5200, NS5400, NS5GT-TRUST-UNTRUST, NSISG1000, NSISG2000, SSG140, SSG20, SSG20-WLAN, SSG320, SSG320M, SSG350, SSG350M, SSG5-ISDN, SSG5-ISDN-WLAN, SSG5-SB, SSG5-SERIAL, SSG5-SERIAL-WLAN, SSG5-V92, SSG5-V92-WLAN, SSG520, SSG520M, SSG550, SSG550M
media-flow	Junos Content Encore	VXA1000, VXA2000
junos-qfx	QFX Series	QFX3500S, QFX3600
junos-qf	QF	QFX3000, QFX3000-G, QFX3000-M
bxos	BXOS	BX7000
tcaos	TCA Series	B-5510, B-5515, B-6010, B-6015, B-7510, B-7515, C-2010, C-2015, C-2020, C-2025, C-2030, C-2035, TCA6000, TCA6500, TCA6K Series, TCA8000, TCA8500, TCA8K Series

Related Documentation

- [Managing DMI Schemas Overview on page 804](#)
- [Setting a Default DMI Schema on page 813](#)
- [Updating a DMI Schema on page 806](#)
- [Troubleshooting DMI Schema Management on page 814](#)

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 installation 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 uses 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 the device and DMI schema. If it does not find a match, it uses the default schema (see [“Modifying the Configuration on the Device” on page 21](#)).

To set a default DMI schema:

1. Select **Administration > DMI Schemas**.

The **DMI Schemas** page appears, 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 is previously used as the default, in tabular view, its cell in the **State** column becomes empty, 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 804](#)
- [Updating a DMI Schema on page 806](#)
- [Creating a Compressed Tar File for Updating DMI Schema on page 809](#)
- [Troubleshooting DMI Schema Management on page 814](#)

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 the 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 discovered devices should be preinstalled. 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 is unsuccessful.

There is no workaround for this problem.

Schema tree not displayed

Typically, if a schema is defective, its schema tree is not displayed.

To verify that a particular schema is parsed successfully:

1. Click the + sign adjacent to **Device Templates**.
2. Select **Definitions**.
3. Click the **Create Template Definition** icon.
4. Select the schema 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 options.

If the topmost node (**Configuration**) cannot be opened to reveal the hierarchy, the schema is corrupted during porting (grep for SchemaMgr ERROR in server.log).



NOTE: One defective schema does not affect other DMI schemas, which are still available for use.

The solution to this problem is to replace one or more existing DMI schemas on the Junos Space server.

To replace one or more existing DMI schemas on the Junos Space server, perform one of the following tasks:

- Use a script supplied by Juniper Networks support. This requires restarting JBoss.
- Use your own .tgz file. This does not require restarting JBoss.

For instructions, see [“Creating a Compressed Tar File for Updating DMI Schema” on page 809](#).

- Related Documentation**
- [Managing DMI Schemas Overview on page 804](#)
 - [Updating a DMI Schema on page 806](#)
 - [Creating a Compressed Tar File for Updating DMI Schema on page 809](#)
 - [Setting a Default DMI Schema on page 813](#)

CHAPTER 76

Generate Key

- [Key-Based Authentication Overview on page 817](#)
- [Generating and Uploading Authentication Keys to Devices on page 817](#)

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 (which uses public-key cryptographic principles). 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 92](#). 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 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.

Junos Space Network Management Platform automates the 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 92](#)

Generating and Uploading Authentication Keys to Devices

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.

- [Generating Authentication Keys on page 818](#)
- [Uploading Authentication Keys to Multiple Managed Devices for the First Time on page 819](#)
- [Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space on page 820](#)

Generating Authentication Keys

To generate a public/private key pair for authentication during login to network devices:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.
The Fabric page is displayed.
2. Click the Generate Key icon on the Actions bar.
The Key Generator pop-up window is displayed.
3. (Optional) In the **Passphrase** field, enter a passphrase to be used to protect the private key, which remains on the system running Junos Space Network Management Platform and is used during device login. 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 impedes an attacker who may gain control of your system and try to log in to your managed network devices.
4. (Optional) Schedule the Junos Space Network Management Platform to generate authentication keys at a later time or immediately.
 - To specify a later start date and time for key generation, select the **Schedule at a later time** check box.
 - To initiate 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 the Junos Space server time but uses the local time zone of the client computer.

5. Click **Generate**.

The Generate Key Job Information dialog box appears, displaying a job ID link for key generation. Click the link to determine whether the key is generated successfully.

Uploading Authentication Keys to Multiple Managed Devices for the First Time

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Click the Upload Keys to Devices icon on the Actions bar.

The Upload Keys to Devices pop-up window is displayed.

3. To upload keys to a single device:

- a. Select **Add Manually**.

The Authentication Details field appears within the Upload Keys to Devices dialog box.

- b. Select **IP Address** or **Hostname**.

- c. In the **IP Address/Host Name** field, enter the IP address or the hostname of the target managed device.

- d. In the **Device Admin** field, enter the appropriate username for that device.

- e. In the **Password** field, 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, CSV file select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

The sample CSV contains the format for entering 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 the “user admin” user on the device.

- c. When 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 a .csv extension.
- e. Click **Upload** to upload the authentication 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 are uploaded and whether this operation is a success.

The green check mark adjacent to the **Select a CSV To Upload** field indicates that the file is 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 managed devices (that were discovered through RSA authentication) in Junos Space, if a new key is generated on Junos Space.

Upload Authentication Keys on Managed Devices that have Conflicting Keys with Junos Space

To upload authentication keys to one or several managed devices manually:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

The Device Management page is displayed.

2. Select the devices to which you want to upload authentication keys and click the Upload Keys to Devices icon on the Actions bar.

The Upload Keys to Devices pop-up window is displayed. The IP address of the devices are prepopulated.

3. In the **Device Admin** field, enter the appropriate username for that device.
4. In the **Password** field, enter the password for that device.
5. Confirm the password by reentering it in the **Re-enter Password** field.
6. Select **Next** to provide details for the next device.
7. Select **Upload** to upload the authentication keys to the managed devices.

The Upload Authentication Key dialog box displays a list of 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 the “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.

**Related
Documentation**

- [Key-Based Authentication Overview on page 91](#)
- [Device Discovery Overview on page 109](#)
- [Discovering Devices on page 111](#)
- [Resolving Key Conflicts on page 95](#)

PART 13

Systems of Record and Disaster Recovery

- [Systems of Record and Disaster Recovery on page 825](#)

Systems of Record and Disaster Recovery

- [Systems of Record in Junos Space Overview on page 825](#)
- [Disaster Recovery Overview on page 826](#)
- [Creating the DR Master Cluster on page 828](#)
- [Creating the DR Slave Cluster on page 831](#)
- [Performing a Reverse Restore on page 836](#)

Systems of Record in Junos Space Overview

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 825](#)
- [Implications on page 826](#)

Systems of Record

A network managed by Junos Space Network Management Platform contains two repositories of information about the devices in the network: the devices themselves (each device defines and reports its official state) and the Junos Space Network Management Platform database (which contains information that is reported by the device 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 operation 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 the contents of 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 operation is executed 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 the device 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. However, if the tester forgets to reset the configuration at the end of the test, 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 to 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. The device notifies Junos Space Network Management Platform via system log when the changes 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. In 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 this process is less efficient.

In the NSOR scenario, you can disable automatic resynchronization. When autoresynchronization is turned off, the server continues to receive notifications and goes into the out-of-sync state; however, autoresynchronization 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 the device's out-of-band changes.

- Related Documentation**
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 17](#)

Disaster Recovery Overview

- [Overview on page 827](#)
- [Prerequisites on page 827](#)

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 828](#).
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 831](#).
3. When your original DR Master comes back online, perform a reverse restore operation to convert the DR Master to a DR Slave. See [“Performing a Reverse Restore Operation” on page 836](#)

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 775](#)). 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 is 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 operations cannot be performed on the same server.
- Backup configuration and restore configuration operations should be performed only on the VIP node of respective clusters. If a VIP switchover occurs, you need to rerun the backup or restore operation (depending on the role) on the new VIP node.



CAUTION: Note that the disaster recovery feature is not supported if the specialized node (FMPM node) is part of a Junos Space fabric. That is, if you have configured a specialized node (FMPM node) on a Junos Space fabric, then you cannot back up or restore the entire configuration because the network monitoring data running on the specialized node is not backed up. The backup includes data present in the VIP node only.

Related Documentation

- [Creating the DR Master Cluster on page 828](#)
- [Creating the DR Slave Cluster on page 831](#)
- [Performing a Reverse Restore Operation on page 836](#)
- [Disaster Recovery Solution and Connectivity Requirements](#)

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 829](#)
- 2. [Starting the Backup for the DR Master Cluster on page 830](#)
- 3. [Stopping the Backup on page 831](#)

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

- [Disaster Recovery Overview on page 826](#)
- [Creating the DR Slave Cluster on page 831](#)
- [Performing a Reverse Restore Operation on page 836](#)

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 832](#)
- [2. Starting to Pull the Backups From the DR Master on page 833](#)
- [3. Stopping Pulling the Backups from the DR Master on page 834](#)
- [4. Restoring on page 835](#)

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/revaliases...

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 host....
```

```
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 host....

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 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**
- [Disaster Recovery Overview on page 826](#)
 - [Creating the DR Master Cluster on page 828](#)
 - [Performing a Reverse Restore Operation on page 836](#)

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 828](#).
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 ["Disaster Recovery Overview" on page 826](#).
3. Configure the new DR Slave site for restore. See ["Creating the DR Slave Cluster" on page 831](#).



NOTE: After you run the restore script, the network monitoring node list might contain previous Junos Space Servers as well.

- Related Documentation**
- [Disaster Recovery Overview on page 826](#)
 - [Creating the DR Master Cluster on page 828](#)
 - [Creating the DR Slave Cluster on page 831](#)

PART 14

Index

- [Index on page 839](#)

Index

Symbols

#, comments in configuration statements.....	xxxi
(), in syntax descriptions.....	xxxi
< >, in syntax descriptions.....	xxxi
[], in configuration statements.....	xxxi
{ }, in configuration statements.....	xxxi
(pipe), in syntax descriptions.....	xxxi

A

AAA	
configuring.....	764
active configuration	
viewing	39
adding Junos Space application.....	721
administration	
smtp server	
add	776
administrators	
CLI.....	619, 620
maintenance mode.....	620
overview.....	619
user interface See user administration	
alarm notification	
configuration overview.....	465
configuring.....	468
alarms	
viewing and managing.....	97, 417
application	
adding.....	721
Platform, adding.....	729
uninstalling.....	733
upgrading.....	725
applications	
managing.....	705
settings, modifying.....	709
auto resync device.....	709
automatic logout of idle user sessions	
(mins).....	709
maximum auto resync waiting time	
(secs).....	709

Applications workspace	
application, adding.....	721
assets	
tracking and searching for.....	405
assigned shared objects	
unassigning.....	35
viewing.....	35
associated scripts	
viewing.....	54
association	
image-device.....	289
script-device.....	319
attribute	
certificate.....	754
audit log	
UTC to local timestamp, converting.....	608
audit logs	
archive file, naming conventions.....	611
archiving and purging.....	611
archiving to local server.....	611
archiving to remote server.....	612
default directory.....	604
exporting.....	615
overview.....	603
tabular view.....	604
user privileges.....	604
viewing	
most active users in last 24 hours.....	608
statistics.....	606
audit logs table	
description.....	604
job ID.....	604
task results.....	604
timestamp.....	604
audit trails	
exporting.....	615
authentication and authorization	
configuring a RADIUS server for.....	764
configuring TACACS+ for.....	768
authentication keys	
generating and uploading.....	92, 149, 817
authentication mode.....	749
authentication modes	
local.....	758
remote.....	758
remote-local.....	758
authentication server	
creating.....	760
modifying.....	763

auto resync device application setting.....	709	CLI configlets	
automatic logout of idle user sessions (mins)		applying to devices.....	76
application setting.....	709	applying to logical interfaces.....	64
automatic resynchronization		applying to physical interfaces.....	63
disabling.....	19	applying to physical inventory.....	62
B		cli configlets	
backup and restore See database		cloning.....	229
braces, in configuration statements.....	xxxi	creating.....	225
brackets		exporting.....	232
angle, in syntax descriptions.....	xxxi	importing.....	230
square, in configuration statements.....	xxxi	modifying.....	231, 262
C		cli configlets statistics	
CA certificate.....	748	viewing.....	234
canceling		comments, in configuration statements.....	xxxi
jobs.....	509	commit script.....	275, 316
certificate		conditions for deleting a fabric node.....	647
attribute.....	754	configlet	
errors.....	750	viewing.....	127
expiry.....	753	configlets	
installing.....	751	downloading.....	127
managing.....	745	configuration change log	
PKCS # 12 format.....	752	viewing.....	31
X.509 format.....	751	configuration file	
certificate revocation list (CRL).....	748	editing.....	482
changing user passwords.....	5, 593	configuration file inventory	
charts		viewing.....	476
viewing.....	429	configuration file management	
Checksum verification.....	290	overview.....	473
checksum verification		user privileges in.....	475
deleting results	360	configuration files	
procedure.....	320	backing up.....	488
verification result page controls		comparing.....	480
description.....	361	deleting.....	477
viewing results	360	exporting.....	484
clearing		restoring.....	478
all my jobs.....	510	updating network monitoring after	
my job.....	510	upgrade.....	433
CLI administrator		configuration filter	
changing password.....	620	creating.....	261
name.....	620	configuration filters	
tasks.....	620	deleting.....	262
cli configlet to devices		configuration guides	
applying.....	228	overview.....	159
cli configlet versions		configuration options	
comparing.....	232	, editing.....	21
		finding.....	183
		configuration views	
		creating.....	249
		deleting.....	251

- modifying.....251
 - overview.....243
 - user roles.....246
 - variables.....244
 - viewing statistics.....252
 - workflow.....244
- configuring application setting.....721
- configuring application settings.....711
- connection profiles
 - cloning.....132
 - creating.....118
 - deleting.....124
 - modifying.....124
- connection status, for managed devices.....15
- consolidated config
 - validating.....28
- conventions
 - text and syntax.....xxx
- curly braces, in configuration statements.....xxxi
- custom labels
 - deleting.....106
 - modifying.....107
- customer support.....xxxii
 - contacting JTAC.....xxxii
- D**
- data collection
 - SNMP
 - turning on and off.....401
- database
 - backup and restore, overview.....684
 - device configuration data.....110
 - device inventory data.....110
- Database
 - restoring from remote file.....694
- database backup
 - default directory.....686
 - deleting files.....698
 - local.....687
 - overview.....685
 - recurrence info, viewing.....510, 699
 - recurring job.....686
 - remote host.....690
 - viewing files.....696
- database reports
 - overview.....397
 - sending.....426
 - viewing.....426
 - viewing pre-run reports.....427
- database restore
 - local.....692, 693
 - overview.....685
- default gateway, changing.....641
- definition states
 - template.....172
- Deleting a Device Image
 - from Junos Space Network Management Platform.....303
- deleting scripts
 - from devices.....328
 - from Junos Space.....315
- deleting user.....590
- Deploying a Device Image293
- device
 - reactivating replacement.....75
 - RMA state.....75
 - troubleshooting.....19
- device association
 - image.....289
 - script.....319
- device authentication
 - changing.....96
- device configuration
 - approving.....25
 - deploying.....25
 - rejecting.....25
- device configuration data.....110
- device connection status.....15
- device discovery
 - inventory and configuration data.....110
 - overview.....109
 - specifying a probe method.....113
 - specifying credentials.....114
 - specifying device targets.....112
 - viewing status.....115
- Device image deployment
 - in-service software upgrade.....293
- Device Images
 - Overview.....273
- device images and scripts overview.....265
- device inventory
 - data.....110
 - exporting.....53
 - overview.....12
- device job failure
 - retrying.....511
- device management
 - overview.....11

device management IP	
adding.....	641
deleting.....	641
device partitions	
creating.....	82
deleting.....	83
modifying.....	83
device statistics	
viewing	40, 155
device templates	
assigning to a device.....	199
auditing.....	202
creating.....	193
deleting.....	198
deploying.....	195
modifying.....	199
overview.....	165
unassigning from a device.....	200
undeploying.....	197
viewing deployment details.....	201
viewing statistics.....	203
workflow.....	170
devices	
changing resync time delay.....	19
connecting to managed devices.....	86
connecting to unmanaged devices.....	87, 89
deleting.....	67
disabling auto-resync.....	19
discovering.....	111
filtering by csv.....	34
logical inventory	110
physical inventory	110
rebooting.....	81
using show commands.....	69
viewing deployment details.....	37
disabling	
script bundle.....	356
disabling scripts.....	324, 326
configuration example.....	324, 326
disabling users.....	581
disaster recovery	
creating the DR master cluster.....	828
creating the DR slave cluster.....	831
performing a reverse restore.....	836
disaster recovery solution	
prerequisites.....	827
understanding.....	827
DMI Schema	
management overview.....	804
DMI schema	
troubleshooting.....	814
updating a.....	806
DMI schemas	
adding.....	809, 813
documentation	
comments on.....	xxxi
domain	
adding.....	564
deleting.....	567
modifying.....	566
overview.....	557
downloading troubleshooting system log files	
using CLI.....	740
E	
enabling	
script bundle.....	355
enabling scripts.....	321
configuration example for a commit	
script.....	322
configuration example for an event script.....	322
configuration example for an op script.....	322
enabling users.....	581
error	
certificates.....	750
event script.....	275, 316
events	
viewing, querying, and acknowledging.....	414
executing scripts.....	331
with JUISE.....	78
expiry	
certificate.....	753
exporting	
operation.....	344
exporting scripts.....	361
F	
fabric	
adding a node.....	635
connection status.....	638
CPU resource.....	638
device connection IP address.....	638
disk space.....	638
load history.....	651
management IP address.....	638
memory resource.....	638

- monitoring node status
 - application logic.....637
 - database.....637
 - load balancer.....637
- node functions
 - availability.....634
 - fault and performance monitoring.....632
 - multinode.....629
 - single node.....628
- node name.....638
- node serial number.....639
- node threshold limit.....629
- overview.....627, 635
- self monitoring.....652
- system health.....649
- fabric node
 - deleting.....647
- failed
 - device, retrying a job on.....511
- fault and performance monitoring
 - specialized node.....632
- font conventions.....xxx
- G**
- getting started assistants, using.....6
 - See also* help, accessing
- H**
- hardware inventory
 - viewing.....41
- help, accessing.....7
 - See also* getting started assistants, using
- hierarchical tags
 - managing.....783
- I**
- icons
 - job status.....500
- image
 - deploying a device.....293
 - device association.....289
- importing
 - operation.....345
- importing scripts
 - overview.....334
 - procedure.....335
- in-service software upgrade.....293
- installing
 - certificate.....751
- inventory page
 - EOL data.....43
 - objects, tagging.....793
- J**
- job
 - parameters.....504
- job status icons.....500
- jobs.....500
 - archiving.....513
 - canceling.....509
 - management overview.....495
 - purging.....513
 - reassigning.....506
 - removing
 - your jobs.....510
 - types.....495
 - viewing
 - scheduled jobs.....500
 - your jobs.....499
 - viewing statistics
 - by execution time.....504
 - by state.....503
 - by type.....503
- JUISE.....78
- Junos Space
 - as system of record.....825
 - user account, creating.....571
- Junos Space cluster
 - disaster recovery.....827
 - creating the DR master cluster.....828
 - creating the DR slave cluster.....831
 - performing a reverse restore.....836
- Junos Space license, managing.....703
- Junos Space software
 - base application.....727
 - hot-pluggable applications.....727
 - network management platform,
 - upgrading.....729
 - upgrade highlights.....727
 - upgrade scenarios.....727
 - upgrading , before you begin.....728
- K**
- key conflicts
 - resolving.....95
- Key SNMP Customized (KSC) Performance reports
 - viewing.....425

Key SNMP Customized (KSC) reports	
creating.....	423
overview.....	397
key-based authentication	
overview.....	91, 149, 817
L	
license	
60-day trial.....	701
generating.....	701
Junos Space, managing.....	703
key file	
generating.....	702
uploading.....	702
license information.....	110
license inventory	
exporting.....	47
viewing.....	47
Linux hardware	
SNMP monitoring.....	667
local authentication mode.....	758
local password	
for remote authentication, clearing.....	594
logging in to Junos Space with remote	
authentication configured.....	770
logging in, to Junos Space.....	3
See also logging out, from Junos Space	
logging out, from Junos Space.....	7
See also logging in, from Junos Space	
logical interfaces	
viewing.....	45
logical systems	
creating.....	71
deleting.....	72
understanding.....	71
login behavior	
remote authentication.....	394, 770
remote-local authentication.....	771
looking glass	
using in Junos Space.....	69
M	
maintenance mode	
actions menu.....	621
administrator name.....	620
administrator password.....	620
administrator tasks.....	620
connecting to Junos Space appliance.....	622
lock time out.....	621
log in screen.....	621
overview.....	621
system locking.....	621
user administration.....	622
manage applications overview.....	705
Manage Applications workspace	
application, uninstalling.....	733
application, upgrading.....	725
Platform, upgrading.....	729
Manage Scripts page	
fields description	276
managed devices	
resynchronizing.....	17, 68
viewing	14
management	
configuration file	
user privileges in.....	475
performance.....	394
management IP	
changing in same subnet.....	641
changing to different subnet.....	641
multinode	
changing in same subnet.....	641
managing applications.....	706
managing Junos Space license.....	703
manuals	
comments on.....	xxxi
maximum auto resync waiting time (secs)	
application setting.....	709
MD5 Validation Results	
Viewing	
Deleting.....	308
model devices	
overview.....	117
modeled instance	
adding.....	122
adding more devices.....	126
viewing.....	125
modeled instances	
deleting.....	131
Modifying Device Image Details.....	307
modifying users.....	587
monitoring	
fabric nodes.....	652
My Jobs feature.....	499
N	
network as system of record.....	825

- network monitoring
 - configuring.....431, 432
 - dashboard, viewing.....403
 - generating log files for troubleshooting.....432
 - interfaces, managing.....441
 - reports
 - overview.....397
 - restarting.....718
 - searching for nodes or asset information.....402
 - services, managing.....441
 - starting.....718
 - stopping.....718
 - updating configuration files after
 - upgrade.....433
 - user privileges.....394
 - viewing and tracking service outages.....413
 - viewing system configuration.....431
 - workspace
 - overview.....394
 - remote authentication login
 - behavior.....394
- network monitoring services
 - restarting.....718
 - starting.....718
 - stopping.....718
- network settings
 - configuration guidelines.....641
 - configuring.....641
- network topology
 - managing alarms.....410
 - pinging nodes.....411
 - viewing alarms by node.....411
 - viewing alarms for nodes.....408
 - viewing events by node.....411
 - viewing history.....407
 - viewing nodes with active alarms.....409
 - viewing resource graphs by node.....412
 - viewing topology map with different
 - layouts.....410
- networking monitoring
 - resyncing nodes.....400
- node
 - adding to fabric.....635
 - definition.....627
 - deleting.....647
 - replacing.....649
 - threshold limit for devices.....629
- node functions
 - application logic.....629
 - database.....629
 - fault and performance monitoring.....632
 - load balancer.....629
- node lists for performance management
 - viewing399
- nodes
 - resyncing400, 825
 - searching for.....402
- notification
 - status
 - configuring network monitoring.....432
- notifications
 - configuring.....446
 - destination paths, configuring.....448
 - event notifications, configuring.....446
 - path outages, configuring.....449
 - scheduled outages, configuring.....449
 - viewing and searching for.....421
- NSOR See network as system of record
- O**
 - object tagging
 - untagging.....794
 - viewing.....794
 - object, inventory
 - applied tags, managing781
 - filtering using tags.....795
 - tag, creating798
 - tags, managing.....780
 - op script.....275, 316
 - operations copying.....342
 - operations creating.....337
 - operations deleting.....343
 - operations exporting.....344
 - operations importing.....345
 - operations modifying.....340
 - operations overview.....281
 - operations running.....341
 - operations viewing.....363
 - out of band changes
 - resolving.....32
 - outages See service outages
- P**
 - parentheses, in syntax descriptions.....xxxi
 - performance See system performance

performance management	
Admin, configuring network monitoring.....	431
notification status.....	432
alarms, viewing and managing.....	97, 417
assets, tracking and searching for.....	405
deleting reports.....	429
event viewing, querying, and	
acknowledging.....	414
notifications, configuring.....	446
notifications, viewing and searching for.....	421
resyncing nodes.....	400
searching for nodes.....	402
surveillance categories, managing.....	463
thresholds, managing.....	441
viewing and tracking outages.....	413
viewing charts.....	429
viewing events.....	415
viewing node lists.....	399
viewing reports.....	424
physical interfaces	
viewing.....	44
PKCS #12 format certificate.....	752
predefined role, managing.....	550
modifying.....	551
Q	
quick templates	
creating.....	206
deploying.....	210
overview.....	205
quick view	
viewing logical systems.....	157
R	
RADIUS authentication methods supported.....	757
RADIUS server	
configuring a	764
reassigning	
jobs.....	506
rebooting nodes.....	646
recurring database backup.....	686
remote authentication	
configuring servers.....	759
Junos Space login behavior.....	770
local password, clearing.....	594
method, selecting.....	759
overview.....	757
password, setting.....	572
server settings, modifying.....	763
server, creating.....	760
remote authentication mode.....	758
remote host	
database backup.....	690, 696
remote-local authentication mode.....	758
removing	
your jobs.....	510
replacing	
node.....	649
report definition	
creating.....	382
managing.....	383
reports	
deleting.....	389
generating.....	387
overview.....	375
resource graphs	
viewing.....	425
viewing.....	388
restoring a database	
overview.....	685
resynchronization	
system of record and	825
Resynchronize with Network command.....	12
resynchronizing See devices	
RMA state	
putting a device in.....	75
role	
predefined, managing.....	550, 551
user-defined, deleting.....	555
user-defined, managing.....	550, 551, 553, 554
role-based administration.....	519
authentication.....	519
enforcement by workspace.....	520
overview.....	519
RBAC enforcement.....	520
RBAC enforcement, limitations.....	520
See also user administration	
roles See user administration	
predefined.....	521
S	
scheduled job statistics	
viewing.....	503
scheduled outages, configuring.....	449
schema	
updating a DMI.....	806

- schema management
 - troubleshooting DMI814
- schemas
 - adding DMI.....809, 813
- script
 - device association.....319
- script bundle
 - device association.....365
 - disabling.....356
 - enabling.....355
- script details
 - Script Details Dialog Box Controls
 - Description.....359
- script modification.....311
- script types
 - modifying.....314
- script versions
 - comparing.....314
- scripts
 - overview.....275, 316
 - user roles.....362
- Secure Console
 - connecting to devices.....86
 - overview.....85
 - terminal control characters.....90
- Secure Copy (SCP) command
 - database backup.....685
- serial number
 - modifying.....80
- server group.....622
- service outages
 - viewing and tracking.....413
- services, network monitoring
 - restarting.....718
 - starting.....718
 - stopping.....718
- SNMP community names, configuring.....440
- SNMP data collection
 - configuring.....440
 - turning on and off.....401
- SNMP MIBs
 - clearing console logs.....452
 - compiling.....451
 - deleting.....451
 - uploading.....450
 - viewing.....451
- software inventory
 - exporting.....51
 - viewing.....51
- software upgrade
 - in-service.....293
- software, Junos Space, upgrading.....724, 727
- SOR See system of record
- specialized node
 - fault and performance monitoring.....632
- SRX device clusters
 - configuring.....137
- SSH session
 - connecting to managed devices.....86
 - connecting to unmanaged devices.....87, 89
- SSoR
 - Space as System of Record.....711
- SSOR See Junos space as system of record
- staged images
 - deleting.....65
- Staging a Device Image286
- states
 - template definition.....172
- statistics
 - audit logs.....606
 - jobs.....503
 - users.....595
- statistics reports
 - generating for export.....428
 - viewing.....427
- status
 - notification
 - configuring network monitoring.....432
- Super Administrator.....521
 - privileges.....521
 - See also user administration
- support, technical See technical support
- surveillance categories, managing.....463
- syntax conventions.....xxx
- system
 - connecting to appliance in maintenance
 - mode.....622
 - database restore.....621
 - debugging.....621
 - performance
 - improving.....513
 - shutdown.....621
- system locking See maintenance mode
- system of record
 - networks as.....711
 - setting.....709
 - Space as.....711
 - understanding.....825

system status log file.....	735
checking, customize.....	737
downloading.....	736
downloading using SCP.....	742
downloading using USB device.....	741
files to download, customize.....	738
system status log file overview.....	735

T

TACACS+	
configuring.....	768
tagging managed objects.....	793
tags	
creating.....	793, 798
deleting.....	791
inventory objects, filtering.....	795
managing.....	780, 781
renaming.....	790
sharing.....	789
untagging.....	794
viewing.....	794
technical support	
contacting JTAC.....	xxxii
template definition	
adding rules.....	181
cloning.....	185
creating.....	173
deleting.....	186
exporting.....	186
importing.....	187
managing CSV files.....	190
modifying.....	188
publishing.....	189, 191
using device-specific values.....	179
viewing statistics.....	171
template definition states.....	172
terminal control characters	
for Secure Console.....	90
thresholds	
creating, modifying, and deleting.....	441
topology See network topology	
troubleshoot zip file	
contents	736, 738
download from Junos Space Network Management Platform UI.....	738
download in maintenance mode.....	740
troubleshooting	
device.....	19

U

unified ISSU.....	293
uninstalling Junos Space application.....	733
unlocking user.....	592
unmanaged devices	
adding.....	133
modifying.....	136
untagging inventory objects.....	794
upgrade	
in-service software	293
upgrading Junos Space application.....	725
upgrading Junos Space Network Management Platform.....	729
upgrading Junos Space software.....	724, 727
Uploading a Device Image	285
user account	
creating in Junos Space.....	571
user administration.....	519
default Super Administrator.....	521
role assignment, understanding.....	521
roles	
definition.....	521
predefined.....	521
task group.....	521
viewing statistics.....	595
viewing user account information.....	582
See also role-based administration	
user certificate.....	747
user privileges.....	172
configuration file management.....	475
user roles	
network monitoring.....	394
user-defined role, creating.....	553, 554
user-defined role, deleting.....	555
user-defined role, managing.....	550, 551
creating.....	551
deleting.....	551
overview.....	551
users	
disabling.....	581
enabling.....	581
history.....	651

V

view script details.....	359
viewing charts.....	429

VIP interface	
changing in same subnet.....	641
changing to a different subnet.....	641
multinode	
changing in same subnet.....	641

W

workspace	
Administration.....	627
administrator access.....	519
Audit Logs.....	603
DMI Schema Management.....	804
enforcement.....	520
Jobs.....	495
Users.....	520
ww adapter	
installing.....	146, 147
wwadapter	
overview.....	145

X

X.509 format certificate.....	751
xpath and regex	
deleting.....	258
modifying.....	258

